MFT 3.4.0.0 Server Configuration Guide

MFT 3.4.0.0 Server Configuration Guide

Publication date 2019-11-05

EquiSign
76 route de la Demi-Lune
Les Collines de l'arche
92057 Paris La Défense Cedex-France
France
www.equisign.fr

Copyright © 2019 EquiSign. All Rights Reserved.

This product, including its related documentation, is protected by copyright and may be protected by patent.

Restricted Rights. This product, including its associated documentation, is intended to be used exclusively by holders of valid EquiSign licenses for the products documented herein. No part of this document may be reproduced or transmitted, in any form or by any means, without the prior written consent of EquiSign.

Limited Liability. While the utmost precaution has been taken in the preparation of this documentation, EquiSign assumes no responsibility for errors or omissions in this documentation. Information in this document is subject to change without notice and does not represent a guarantee on the part of EquiSign. The documentation is provided "as is" without warranty of merchantability or fitness for a particular purpose. Furthermore, EquiSign does not warrant, guarantee, or make any representations regarding the use, or the results of the use, of the documentation in terms of correctness, accuracy, reliability, or otherwise.

Trademarks and Trade Name. EquiSign® is a registered trademark of EquiSign SAS in the United States and other countries. EquiSign is a trade name of EquiSign SAS in the United States and other countries.

All other brand or product names referred to in this document are registered trademarks, trademarks, service marks, or trade names of their respective owners.

Third-party Reference Documentation. The information contained in this document is not yet part of the standard EquiSign documentation set or is intended to be a reference guide for integrating EquiSign products with third-party software. As such, it is not officially supported or maintained by EquiSign and will not necessarily be updated on the same release schedule as officially supported EquiSign products and their associated documentation.

Pre-release Documentation. The information contained in this document is not yet part of the standard EquiSign documentation set or is intended to be a reference guide for integrating EquiSign products with third-party software. As such, it is not officially supported or maintained by EquiSign and will not necessarily be updated on the same release schedule as officially supported EquiSign products and their associated documentation.

Supplemental Documentation. The information contained in this document is not yet part of the standard EquiSign documentation set or is intended to be a reference guide for integrating EquiSign products with third-party software. As such, it is not officially supported or maintained by EquiSign and will not necessarily be updated on the same release schedule as officially supported EquiSign products and their associated documentation.

Developer Documentation. The information contained in this document was written for developers by developers as a reference tool. It will not necessarily be updated on the same release schedule as EquiSign products and their associated documentation.

Table of Contents

Preface vi
1. Resources vi
1.1. Contact Customer Service vi
1.2. Contact Professional Services vi
1.3. Provide Documentation Feedback vi
2. Document Conventions vi
1. Conceptual Overview 1
1.1. Domains 1
1.2. Users 1
1.3. Exchanges 1
1.4. Policies 2
2. Configuration Overview 3
3. Configure Domains 4
4. Configure Authentication Mechanisms 9
4.1. Configure an LDAP Directory Connection 10
4.2. Configure Authentication or Contact Source Plug-ins 11
4.3. Customize Login 14
4.4. Configure Authentication Policies 16
5. Manage Users 18
5.1. Create Tags 18
5.2. Add, Edit, and Delete Individual Registered Users 19
5.3. Add and Synchronize Registered Users By File Upload 21
6. Manage Rights 22
6.1. Configure Groups 22
6.2. Configure Rights 23
7. Configure PDF Document Signing 25
7.1. Manage Trusted Certificates for Signing 25
7.2. Configure Keypairs 26
7.3. Add/Configure PDF Signature Policies 27
8. Configure At-rest Encryption 33
8.1. Manage KeyPairs for at-rest encryption 33
9. Configure Settings 35
9.1. Configure Domain Policies 35
9.1.1. Add/Configure User Quota Policies 36
9.1.2. Add/Configure File Filtering Policies 36
9.1.3. Add/Configure Password Policies 37
9.1.4. Add/Configure Sending Policies 39
9.1.5. Configure Pre-Archiving 41
9.2. Configure Exchange Settings 43
9.2.1. Create an Exchange Rule 43
9.2.2. Create an Exchange Policy 45
9.3. Create/Upload Themes 47
9.3.1. Create a Theme 47
9.3.2. Upload a Theme 50
9.4. Configure Repositories 51
9.4.1. Configure User Providers 51
9.4.2. Configure Datasources 53
9.4.3. Configure Contact Sources 54
9.5. Configure Additional Settings 55
9.5.1. Add/Configure Information Messages 55
9.5.2. Add/Configure Email Templates 56
9.5.3. Manage Scheduled Jobs 60
10. Reporting and Audit Logs 61
10.1. Reporting 61
10.1.1. View User Reports 61

10.1.2. View Activity Reports 62
10.2. Use the Audit Logs User Interface 63
10.2.1. Search for Log Entries 63
10.2.2. Download the Audit Log Files 64
11. Renew Web Server Certificates 65

List of Tables

4.1. SMS provider settings 12

Preface

The following sections contain preface information:

- Section 1, “Resources”
- Section 2, “Document Conventions”

1. Resources

Please use the information provided to contact the appropriate EquiSign department or representative.

1.1. Contact Customer Service

Support Web Site, including the Support Download Site	`https://support.equisign.fr/` (Login requires a username and password)
Email	`<support@equisign.fr>`

1.2. Contact Professional Services

Email	`<support@equisign.fr>`

1.3. Provide Documentation Feedback

As part of an ongoing process to create documentation that is easy to understand and use, as well as relevant to audience roles as administrator users, we welcome feedback about this guide. Please email any comments or suggestions to: `<support@equisign.fr>`

2. Document Conventions

EquiSign documentation uses typographical conventions with specific meanings. These conventions are described in the following table.

Convention	How It Is Used
bold	Indicates the most important part of a step in step-based instructions. Example: Click the OK button.
italic	Indicates a reference to another document or guide. Example: See the Release Notes. Indicates the name of an access right. Example: The unlock right allows an administrator to help an end user unlock a smart card.

Convention	How It Is Used
`monospaced font`	Indicates a file name, directory name or path, code examples and elements, application output, and user-entered text. Example: Save the file in the `/webserver` directory.
`italicized monospaced font`	Indicates an environment-specific or implementation-specific variable. Example: Save the file in the *`root_directory/`*`webserver` directory.
Important:	Contains important information that must be paid attention to. Failure to do so may have a negative impact on the application.
Note:	Contains valuable supplementary information.
Tip:	Contains helpful information that may be useful, for example, a shortcut or another way of performing a task.

Chapter 1. Conceptual Overview

The Managed File Transfer application provides a secure platform in which centralized control of electronic exchanges ensures the traceability and confidentiality of all exchanged data. The Managed File Transfer application uses two interfaces - one for end users and one for administrators, each accessed via separate URLs. In the administration application, administrators can create domains, add and configure users, define message exchange rules and policies, assign rights, and manage the system settings. In the end user application, users send and receive messages from other users.

This guide is intended to be used by Managed File Transfer administrators who have been granted access rights to configure:

- Section 1.1, “Domains”
- Section 1.2, “Users”
- Section 1.3, “Exchanges”
- Section 1.4, “Policies”

1.1. Domains

Users of the Managed File Transfer application can group users into domains or can group all users in a single domain. For example, a domain could be created for users within a country, a company, a specific company branch, or an organizational unit. Domains allow administrators to assign equal privacy and security settings to groups of users by configuring and applying settings such as policies, exchange rights, and user authentication modes on a per domain basis. Administrators can create and edit a theme for a domain, which customizes the graphical appearance of the end user application for the given domain. Administrators can also create a quota for a domain, to control the level of stored information for the domain. Organizing users into domains gives administrators the option to restrict documents exchanges to be within a particular domain or allow wider communication between domains. After domains are created, administrators can assign domains to users (one domain per user).

1.2. Users

The Managed File Transfer application is available to registered users of the Managed File Transfer application as well as guest users. Registered users are users that administrators with the User Management right have added to the Managed File Transfer application and for whom administrators have configured exchange rules and policies. Guest users are non-registered users that registered users can send messages to and who can be given access to the upload function of the Managed File Transfer end user application upon receipt of upload/download tokens from registered users. Users interact with each other through messages exchanges; a message contains one or more documents.

1.3. Exchanges

Users can exchange messages that contain documents in two different ways. One user can send messages to one other user through a simple message or registered users can be grouped into projects to create an efficient and convenient way to send messages within a specific group of

users (a workgroup). If registered users are not added to a project, they will be still be able to send simple messages. Simple messages are single, one time messages that can be sent from one user to other user(s), similar to an email exchange.

1.4. Policies

Policies allow administrators to determine how users and guest users can interact with the Managed File Transfer application and with each other. Some policies can be applied to an entire domain, or to individual users, or to both domain and users. All types of policies essentially work in the same way. An administrator with the appropriate rights creates a policy and then applies the policy to a selected domain or user. During the configuration process, the administrator selects the scope of the policy. The scope of all policies can be defined as "global to all domains" or "local to a domain." Policies that are global to all domains are visible and available for use with all domains and can be configured by an administrator with the Global Settings Management right. Local policies are visible and available for use within a single domain and can be configured by an administrator with the Local Settings Management right for the selected domain or with the Global Settings Management right. Once configured, a policy can be applied to a domain or a user by editing the configuration properties for the domain or user.

Chapter 2. Configuration Overview

The configuration of the Managed File Transfer administration application is separated into instruction processes that have been organized by the order in which they should be followed. During the initial configuration process some components, such as the domains, must be configured with a minimum-level of customization, then returned to and fully configured later after creating and configuring other elements, such as those in the Settings section. In this way, the guide is designed to follow the logical order of the initial configuration process, but to also enable administrators to be able to return to configuration instructions to perform updates and editing or to create customizing aspects after the initial configuration setup. During the installation process several key components of the Managed File Transfer administration application will be automatically installed. These include the "admin-mft" administrator, the MFT Domain, and the default Authentication Profile, Theme, Sending Policy, User Quota Policy, and Password Policy.

- Chapter 3, Configure Domains - During the initial configuration process, the administrator configuring the system should first determine how many domains will be needed. While most installations will only require one general domain, administrators can configure as many domains as are allowed by the license. If more than one domain is necessary, configuring the additional domains should be the first step in the configuration process. The Managed File Transfer Domain can be edited and customized by an administrator or a new domain can be created to replace the Managed File Transfer Domain.

- Chapter 4, Configure Authentication Mechanisms - The authentication process should be configured during the initial configuration process. The authentication configuration instructions contains instructions on how to configure and assign authentication specifications. During the initial configuration process, the authentication configuration instructions should be completed before other configurations so that users can be created and given the ability to authenticate to the system to configure other settings. At any time after the initial configuration, an administrator with the appropriate rights can add new authentication specifications to allow newly added users to authenticate to the system in a different manner if it is necessary.

- Chapter 5, Manage Users - Users can be created, edited, and assigned rights continuously by an administrator with the proper rights. Therefore, during the initial configuration process, only those users that will be given high-level administrator rights need to be configured. A full list of users can be created later. This will limit the amount of editing required by the administrators as well as allow an administrator that corresponds to a physical person to have access to the system with administrative rights as early into the configuration process as possible. It is recommended to create at least one administrator or group with rights equal to the "admin-mft" administrator during the initial configuration process, but several can be created if necessary. Rights for either individual users or groups of users can be assigned and edited continuously as needed, as described in Chapter 6, Manage Rights.

- Chapter 9, Configure Settings - Policies are created to customize domains and users. The policies within the settings configurations can be continuously created, edited, and assigned to users or domains throughout use of the Managed File Transfer administration application. This allows the administrator to customize domains and users. Policies and other settings can be created and configured whenever necessary. To apply a policy or setting, see the configuration information for domains and users.

- Chapter 10, Reporting and Audit Logs - The Audit function allows administrators with the Reporting right to search and compile reports on users. Administrators with the Audit Logs right can search and analyze audit logs on the audit log interface.

Chapter 3. Configure Domains

A domain is an entity representing both a sphere of administration and of document exchange, which thus allows for both the separation of the administrative access rights needed to manage users or policies, and the control of documents exchanged between entities. A domain does nolot represent a preset standard unit. A domain could be a company, a business unit, an organizational unit, a practice group, etc. In the event that users need to be separated into different administrative spheres, administrators can create more than one domain. Smaller organizations may choose to leave the basic, built-in options applicable to all users, thus creating one unified domain for the entire system. If this is the case, the administrator can either reuse the default domain, or create a new one and delete the initial default domain. All users belong to only one domain and all policies that are not global to all domains, are associated with only one domain and cannot be used within another domain.

Administrators with the Domain Management right can create and configure as many domains as needed and edit any properties of any domain. Administrators with the Local Settings Management right are allowed to edit the General and Notification properties of existing domains.

During the initial configuration process, several parameters will not be configurable because of settings configuration dependencies. The domain can be created and configured with minimal customization, then edited in the same way after settings are configured, as described in Chapter 9, Configure Settings.

Procedure 3.1. To configure a domain:

1. Log in to the Managed File Transfer administration application as an administrator with the Domain Management right or the Local Settings Management right.
2. Navigate to the Settings | Domains | Domains page.
3. On the Domains page, choose to Create a New Domain or to Modify or Remove an existing domain.
4. If the choice is to create a new domain or to modify an existing domain, on the General tab, configure the following general domain settings:
    a. Name,Company and Description - Enter a name, an optional company name and an optional description for the domain. The name will be visible in other parts of the user interface for the administration application. Providing detailed information in the name and description fields will make it easier to select the correct domain in other parts of the user interface for the administration application.
    b. Short Application Name - From the drop-down menu, choose to keep the default application name (as globally configured in the Advanced Settings page as client.product.appname.short) or to give the application a custom name visible for the domain users. If the choice is to give the application a custom name, in the text box, enter the short version. The short version of the application name will be displayed in the title of the end-user application Web pages, and is also available for selection when configuring mail templates as described in Section 9.5.2, “Add/Configure Email Templates”.
    c. Full Application Name - From the drop-down menu, choose to keep the default application name (as globally configured in the Advanced Settings page as client.product.appname.full) or to give the application a custom name. If the choice is to give the application a custom name, in the text box, enter the full version. The full application name is available for selection when configuring an email template as described in Section 9.5.2, “Add/Configure Email Templates”. It is typically used in the signature of email notifications.

d. Administrator Email - From the drop-down menu, choose to keep the default contact email address (as globally configured in the Advanced Settings page as contact.administrative.email) or to enter a custom contact email address. If custom contact email address is selected, enter the email address that will serve as the contact email address for the domain. The domain contact receives email if the platform is configured to send notifications when an uploaded document could not be validated (typically because it contains a virus). See in the Advanced Settings the configuration keys whose prefix is file.validator for the complete list of document validation mechanisms. The domain contact also receives notifications when the domain's global disk space quota is about to be reached. The contact email address is also available for selection when configuring an email template as described in Section 9.5.2, “Add/Configure Email Templates”, typically for the notification sent when a user asks for more quota.

e. Administrator Name - This feature is not used for the moment, and can thus be ignored.

f. Default Language - From the drop-down menu, select the language to use for emails to users whose language is unknown. The default language will be used when the negotiated user language is not specified or when choosing a language not available when configuring a mail template. It is thus important that configured email templates provide text in this default language.

g. Message of the Day - From the drop-down menu, select a message of the day. The Message of the day is displayed to all end users within the domain when they log in to Managed File Transfer. All information messages of the day that have been configured to be available to the domain will be available for selection, as described in Section 9.5.1, “Add/Configure Information Messages”. From the drop-down menu, select None if a message of the day is not needed for this domain.

h. Theme - From the drop-down menu, select a theme. All themes that have been configured as available to the domain will be available for selection. If a unique theme has not yet been configured, as described in Section 9.3.2, “Upload a Theme”, the default theme will be used. The theme selected will be visible on the end user application to all users within the domain and will also be visible to guest users of the domain.

i. Default Authentication Policy - From the drop-down menu, select the authentication policy to select by default when creating a new user within the domain. All authentication policies that have been configured as available to the domain will be available for selection, as described in Section 4.4, “Configure Authentication Policies”. Important note: the selected authentication policy is attached to users automatically created via the User Provider mechanism, as described in Section 9.4.1, “Configure User Providers”.

j. Inactive Users Deletion - Check to set the period after which inactive users are deactivated (Deactivation after). Deactivated accounts will be definitively removed once the grace period (Definitive deletion after) is expired. Users deletion can be processed either manually or scheduled at a specific moment depending on the configuration of the CleanInactiveUsers job (see Section 9.5.3, “Manage Scheduled Jobs”).

k. Password Aging - Check to force users to set a new password after a specified period (90 days by default). If this option is checked, set the validity period of users' password in the Password Validity Duration field. In addition - from the Change Password Title drop down menu - select the message that is displayed to users when they are prompted to change their password. All information messages that have been configured to be available to the domain will be available for selection, as described in

Section 9.5.1, “Add/Configure Information Messages”. Users whose password is to be changed cannot reuse their latest password.

l. Default Exchange Policy - From the drop-down menu, select the exchange policy to select by default when creating a new user within the domain. All exchange policies that have been configured as available to the domain will be available for selection, as described in Section 9.2.2, “Create an Exchange Policy”. Important note: the selected exchange policy is attached to users automatically created via the User Provider mechanism, as described in Section 9.4.1, “Configure User Providers”.

5. On the Notifications tab, configure the following domain notifications settings:

   a. Message Expiration Notifications - When a message is about to expire, two warning emails will be sent to the recipients of the message who have not yet downloaded all the message's documents. Enter a value or use the up and down arrows to configure the number of days before the message expiration date that each notification email should be sent.

   b. Email Sending Configuration - When the Use Specific Configuration option is selected, the origin path of all emails sent from this domain can be configured. This will control what appears in the return path, sender, and from headers. If not selected, the global configuration will be used. Email sending configuration may be needed when working under a server that imposes restrictions or for overcoming anti-span mechanisms. To configure the origin path of emails, select to Use Specific Configuration and configure the following specific configuration options:

      i. Mail Fixed Sender - In the text-entry box, enter the email address to appear as the value of the return-path and as the sender header of all emails sent by the Managed File Transfer via this domain.

      ii. Mail Sender Strategy - From the drop-down menu, select one of the following email sender strategies to define the 'From' and 'Replyto' headers of emails sent from this domain:

         A. Use the mail template configuration - Select this option to use the value configured in the 'From' header of mail template attached to this domain.

         B. Use fixed email address - Select this option to use the fixed email address set in the Email Fixed Sender option for the 'From' header.

         C. Use fixed email address and set a 'Replyto' - Select this option to use the fixed email address set in the Mail Fixed Sender option for the 'From' header and to use the value configured in the 'Reply-To' header of the mail template attached to this domain.

   c. Mail Notifier - From the drop-down menus, select the appropriate email template for each event. Email templates created in Section 9.5.2, “Add/Configure Email Templates” for the event corresponding to the drop-down menu will be displayed. If an email template has not yet been configured, this option can be edited after settings are configured. Several email templates can be associated with the same event if they have been created and configured for the event.

6. On the Quota tab, configure the following domain and user quota settings:

   a. Domain Quota - To enable a domain-wide quota, select Apply Quota to Domain. Enabling a domain-wide quota imposes a limit on the combination of the total storage size of all users of the domain and of all upload tokens created by users of the domain. If the option to apply a domain quota is selected, enter a value or use the up and down arrows to configure the quota size in MB.

b. Warning Threshold - If the storage size reaches this threshold, an email is sent to the domain administrator (see the General tab above).

c. User Quotas - To enable user quotas, select Use User Quotas on Domain. When user quotas on a domain are enabled, all domain users must have a quota policy explicitly attached to them. When the domain is saved, the Default User Quota Policy is thus automatically attached to all users of the domain who do not still have a quota policy.

   At least one quota policy must have been created before selecting this option so that the Default User Quota can be defined.

d. If the Use User Quotas on Domains option is selected, continue to the next step. If the Use User Quota on Domains option is not selected, continue to the Advanced tab.

e. Maximum User Quota Value - Enter a value or use the up and down arrows to configure the maximum quota size in MB. The Maximum Quota Value represents the maximum size that quota policies can be created for and attached to users within this domain. Setting a maximum quota value ensures that administrators with the Local Domain Management right for this domain will not be able to create a quota policy that exceeds the set maximum quota value.

f. Default User Quota Policy - From the drop-down menu, select the quota policy that will serve as the default quota for each user within the domain (see Section 9.1.1, “Add/ Configure User Quota Policies”). The quota policy selected as the Default User Quota will be selected by default when creating a new user within the domain. If users within the domain have already been created, editing this option will apply the default user quota to all users that have not been previously configured to have a user quota policy.

g. Allows Users to Request Quota Increase - To enable users to request a higher quota, select this option. If enabled, a "Request Quota Increase" link will be displayed to the user in the end-user application. Depending on the configuration of notifications and mail templates, an email can be sent to the domain administrator to notify a quota increase request.

7. On the Advanced tab, configure the following advanced domain settings:

   a. URL - Enter the end user application URL to be used in email messages that contain a link to the end user application. Configuring a new domain URL is an optional step and will override the default public URL as defined in the original installation settings and visible on the Advanced Settings page as access.public.url. If custom URL is selected, it can be selected to allow the default public url to continue to be used for guest users when they are sent mail.

   b. User ID Regex - From the drop down menu, select to use the default user ID regular expression, or a custom user ID regular expression. If a custom user ID regular expression is selected, enter it into the text box. Upon user creation, the UID of the user must match this regular expression. Use the keyboard icon to test the validity of the custom regular expression. The User ID Regex will be visible on the Advanced Settings page as adminclient.user.uidRegex.

   c. Limit User Count - Enables a limit of the amount of users added to the domain to be imposed. If selected, enter a value or use the up and down arrows to configure the Maximum Number of User Accounts.

   d. Login Type - From the drop-down menu, choose the type of login prompt that will be displayed to the user when logging into the Managed File Transfer administration application:

- Unified Login Prompt - The user will be prompted to enter both their login ID or email address and password at the same time.

- Separate Identification and Authentication Phases - The user will first be prompted to enter the individual login ID or email address on an initial page, then will be directed to a second page to enter their password. By first identifying the user, the Managed File Transfer application is able to determine which authentication criteria the user must provide to access the application (see also Section 9.1.3, “Add/Configure Password Policies”). For example, some users will need to provide a password while others might be asked to provide a one-time password. In most cases the identification and authentication phases do not need to be separated.

e. File encryption method - From the drop-down menu, choose the file encryption method that will be used for the users of this domain:

   - Cyphered ZIP (default) - Files will be encrypted as a 7ZIP file with the AES256 algorithm. Recipients can decrypt the files using a compatible 7ZIP extractor, e.g. 7Zip on Windows or Keka on MacOS.

   - Cyphered ZIP (default) - Files will be encrypted as a ZIP file with the AES256 algorithm. Recipients can decrypt the files using a compatible ZIP-AES256 extractor, e.g. 7Zip on Windows or Keka on MacOS. Please note that the default ZIP extractors on Windows and MacOS do not support AES256-encrypted ZIP files.

f. Contact Source - From the drop-down menu, select a contact source. The drop-down menu is populated by contact sources that have already been configured, as described in Section 9.4.3, “Configure Contact Sources”. If a contact source has not yet been created, this option can be edited after contact source plug-ins are configured. The contacts belonging to the selected source will be displayed in the auto-suggestion dialogs (namely when choosing the recipients of a new message.)

g. Sending Policy - From the drop-down menu, select a sending policy. The drop-down menu is populated by sending policies that have already been configured, as described in Section 9.1.4, “Add/Configure Sending Policies”. The selected sending policy will be applied to all "Simple Messages" sent by registered users as well as all messages sent using upload tokens created by a registered user within this domain. Sending policies that govern project messages are applied when the project is created. Select the default sending policy if a custom sending policy has not yet been configured.

8. When all tabs have been configured, click OK.

Chapter 4. Configure Authentication Mechanisms

Each registered user of the Managed File Transfer application must be authenticated to be able to access the application. An authentication mechanism is applied to each user by associating the user with an authentication policy. The Managed File Transfer application provides the following authentication mechanism options:

- The user's login and password is verified based on the internal Managed File Transfer user repository.
- The authentication process is delegated to an external LDAP directory with connection parameters that are configured through an LDAP Directory Connection in the Repositories administrator menu.
- The user is verified by an X509 SSL client certificate.
- The user is verified by an OTP code sent by text message.
- The authentication process is delegated to an external SSO infrastructure, such as CA Technologies SiteMinder.
- SAML 2.0 can be used to authenticate users.

The possibility to authenticate using an internal login and password is provided by the built-in authentication scheme of the Managed File Transfer application. Other authentication schemes can be configured by creating plug-ins, and then attach them to authentication policies, which in turn are attached to user accounts. Using a login/password based authentication scheme is an interactive login method (internal repository, LDAP, SAML), while the other authentication methods are non-interactive (X509, SSO, SAML). Selecting a non-interactive method for an authentication scheme will affect end-user application options such as if the user is able to manually logout of the system via an on-screen option. To allow non-interactive authentication schemes to function in an interactive capacity, configure the corresponding plug-in options.

Each registered user is subject to an authentication policy composed of one or two authentication schemes: a primary authentication scheme and an optional alternate authentication scheme. The alternate authentication scheme can be activated on demand by a help desk administrator who edits the user properties in the Managed File Transfer administration application for the user (or via the Administration SOAP/REST Connectors). The alternate authentication scheme is typically weaker than the primary authentication scheme and is only activated when the user cannot use the primary authentication scheme to access the Managed File Transfer application. For example, a user may have to wait for a new smart card to be issued if the user's primary authentication scheme requires a smart card and the user loses the smart card. In this instance, the user will be able to authenticate with a login and password via the alternate authentication scheme based on the internal Managed File Transfer user repository.

Administrators with the Global Settings Management right have the ability to configure global or local authentication policies, as described in Section 4.1, “Configure an LDAP Directory Connection” and Section 4.4, “Configure Authentication Policies ”. Administrators with the System Setup rights have the ability to configure authentication schemes, as described in Section 4.3, “Customize Login” and Section 4.2, “Configure Authentication or Contact Source Plug-ins”. Administrators with the Local User Management right have the ability to apply an authentication policy to a user belonging to the domain they have the local rights to.

The MFT application also includes a brute-force protection feature that, when activated, is applied system-wide to every configured domain and to each password-based authentication

mechanism, meaning the brute-force protection could be applied, for example, to an authentication mechanism that includes an internal repository, an LDAP directory connection, and a user provider. Administrators can enable this feature and configure the number of failed authentication attempts that will result in a user account being temporarily locked as well as the duration of the temporary lock period on the Server Management | Setup | Advanced Settings page of the UI, on the Base tab, in the "bfp" section.

4.1. Configure an LDAP Directory Connection

LDAP v3 Directories can be used by the Managed File Transfer administration application to authenticate users. LDAP Directory Connections are required to create LDAP authentication schemes and therefore should be configured before attempting to configure an LDAP authentication scheme. Administrators with the Global Settings Management right can configure an LDAP directory.

Procedure 4.1. To configure an LDAP directory connection:

1. Log in to the Managed File Transfer administration application as an administrator with the Global Settings Management right.
2. Navigate to the Settings | Repositories | Directories page.
3. On the Directories page, choose to Create a New LDAP Directory Connection or to Modify, Copy, or Remove an existing LDAP directory connection.
4. If the choice was to create a new LDAP directory connection or to modify an existing LDAP directory connection, on the create a new LDAP directory connection page, configure the following LDAP directory connection options:
    a. Name and Description - Enter a name and description for the LDAP directory connection. The name will be visible in other parts of the user interface for the administration application, for example, when selecting which LDAP directory to use for a particular authentication scheme. Providing detailed information in the name field will make it easier to select the correct LDAP directory in other parts of the user interface for the administration application.
    b. Scope - Choose to make the LDAP directory available to all domains or available to a single domain by selecting Global or Local to a Domain. If local to a domain is selected, select a domain from the drop-down menu.
    c. Connection Type - Choose the security protocol to use when the Managed File Transfer administration application connects to the LDAP directory:
        - Plain - Non-secured connection
        - SSL or TLS - SSL and TLS are both encrypted connections. Choose the type of connection that corresponds to the encryption method configured on the LDAP server.
    d. Host - Enter the fully-qualified domain name of the machine hosting the LDAP directory. To enable fail over use the plus and minus icons to configure the appropriate number of LDAP directory hostnames. An additional host would be used only in the case that the primary host was down or could not be accessed.
    e. Port - Enter a value or use the up and down arrows to enter the LDAP port number on the server hosting the LDAP directory that the Managed File Transfer administration application should use for connections. If several hosts are configured, the same port must be used by each host.

f. Base DN - Enter the Base DN of the LDAP directory. All users must be located under this DN.

g. Authentication Type - Choose the type of authentication to use when authenticating the Managed File Transfer administration application to the LDAP directory:

- None - No authentication is performed. The Managed File Transfer application sends anonymous requests to the external LDAP directory.
- Password - The Managed File Transfer application authenticates using a Bind DN and the password for the Bind DN. If this option is selected, continue to the next step. If not, skip to Step 5.

h. If Password was selected for the Authentication Type, configure the following properties:

- Bind DN - The Bind DN corresponds to an account configured in the LDAP directory for a user. Using the Bind DN, the Managed File Transfer administration application is allowed to search the LDAP directory for Managed File Transfer administration application users.
- Bind Password - Enter the password that corresponds to the Bind DN.

5. To configure advanced LDAP directory options, click Advanced and configure the available advanced options:

a. Bypass Server Certificate Authentication - This option will only be available if either SSL or TLS was selected as the connection type. If this option is selected, the server certificate of the LDAP Directory will not be verified against a certificate hierarchy. Selecting this option may be useful if the Managed File Transfer application's trust store does not contain the LDAP server certificate hierarchy. Be aware that bypassing the server certificate authentication may result in security risks.

b. Bypass Server Hostname Authentication - This option will only be available if TLS was selected as the connection type. If selected, the server hostname will not be checked against the one declared in its certificate. This may be useful to access a server via a non standard IP address or hostname.

c. Automatically Follow References to other LDAP Servers - Select this option to allow the Managed File Transfer application to automatically follow LDAP referrals when the LDAP directory structure is distributed on separate servers.

d. Timeout - Enter a value or use the up and down arrows to configure the number of milliseconds that the server will wait while attempting to connect to the LDAP directory before declaring the connection unreachable.

6. To verify that the settings have been entered correctly and the LDAP directory is accessible, click Test Connection.

7. Click OK.

4.2. Configure Authentication or Contact Source Plug-ins

An administrator with the System Setup right has the ability to configure authentication scheme plug-ins. Authentication schemes are configured by adding authentication plug-ins to the

Managed File Transfer application. Plug-ins are then attached to authentication policies, which in turn are attached to users.

The Managed File Transfer application supports the following types of authentication schemes; internal authentication, OTP, LDAP, SSO, X509 certificate, SAML (interactive and non interactive mode), and simple SQL. Custom authentication scheme plug-ins can be developed to meet specific customer needs. To learn more about custom authentication scheme plug-ins, contact an assigned Equisign technical representative.

Procedure 4.2. To configure an authentication or contact source plug-in instance:

1. Log in to the Managed File Transfer administration application as an administrator with the System Setup right.

2. Navigate to the Server Management | Setup | Advanced Settings page.

3. On the Advanced Settings page, select the Plug-ins tab.

4. Click Add New Properties.

5. From the drop-down menu, select an authentication plug-in instance configuration template:

   - OTP -Use the OTP plug-in to authenticate Managed File Transfer users with a one time password sent by text message. The plug-in only manages authentication, it does not create Managed File Transfer user accounts on the fly; user accounts must have been previously created. To set up an OTP authentication plug-in, ensure also that:

     - OTP Authentication is selected as your domain(s) authentication scheme (see MFT Server Configuration Guide);

     - the type of login is "Separate Identification and Authentication Phases" (see also MFT Server Configuration Guide);

     - a password policy exists (see MFT Server Configuration Guide);

     - registered users have a valid mobile phone number set in Managed File Transfer (see MFT Server Configuration Guide);

     - (if required) a valid proxy is configured to redirect the HTTP requests to the SMS (Short Message Service) provider;

     - the SMS provider properties are correctly configured (see Server Management | Setup | Advanced Settings | BASE).

       ### Table 4.1. SMS provider settings

Property	Description
sms.esendex.account	Account reference provided by the SMS provider to your organization.
sms.esendex.login	Identifier provided by the SMS provider to your organization.
sms.esendex.password	Password provided by the SMS provider to your organization.

     Note that OTP codes are valid for a period of 24 hours from the date they are sent.

- LDAP -Use the LDAP plug-in to delegate Managed File Transfer authentication to an external LDAP v3 directory server (such as Microsoft Active Directory). The plug-in only manages authentication, it does not create Managed File Transfer user accounts on the fly; user accounts must have been previously created. To configure an LDAP authentication plug-in, refer to the online help provided in the plug-in tooltips.

- SSO - Use the SSO plug-in to delegate Managed File Transfer authentication to an external Web SSO infrastructure (such as CA Technologies' SiteMinder). The plug-in only manages authentication, it does not create Managed File Transfer user accounts on the fly; user accounts must have been previously created. To configure a SSO authentication plug-in, refer to the online help provided in the plug-in tooltips.

- X509 Certificate - In order to use an X509 certificate plug-in for authentication, an administrator must manually add the trust chain of certificates and CRLs to the front-end Web servers, using the `/opt/opentrust/mft/sbin/trust-management` tool, and configure the Web servers to enable X509 authentication using the `/opt/opentrust/mft/sbin/mft-config` tool. If the authentication type was configured as optional during installation, an X509 certificate plug-in can be used with other authentication schemes. Exclusively using an X509 plug-in for authentication is not recommended as this will eliminate the option to fall-back on the user/login authentication type.

- SAML - The SAML authentication mechanism is based on the standard SAML 2.0 protocol and supports SAML authentication only. SAML authorization and user account federation are not supported. MFT acts as a SAML Service Provider (SP), delegating authentication to a SAML Identity Provider (IdP). MFT does not need a direct network access to the IdP; all interactions between MFT and the IdP are performed through the user's browser.

  The following MFT configurations are pre-requisites for using the SAML plug-in:

  1. The plug-in only manages authentication, it does not create Managed File Transfer user accounts on the fly; user accounts must have been previously created.

  2. The MFT user accounts and the SAML identity provider user accounts must share a common attribute (usually a UID or an email address) to enable account mapping.

  For technical reasons, the resulting MFT SAML login process is composed of two-steps: The user is first identified in MFT and must provide a UID or email address but no password on the MFT login page. The user is then redirected to the identity provider to authenticate. The two-steps login process can be configured either system-wide to every configured domain (see MFT Server Configuration Guide), or per domain (see MFT Server Configuration Guide).

  MFT supports a subset of the SAML "Web Browser SSO Profile" functionalities:

  - when sending authentication requests to the identity provider, the "HTTP-Redirect" and "POST" bindings, but not artifacts, are available

  - when receiving authentication responses from an identity provider, only the "POST" binding is supported

  - authentication requests and responses may be signed

  - metadata are not supported; a service provider metadata file may be created on demand if requested by the identity provider, but metadata files are not required from the identity provider

  For security reasons, SAML Configuration in Interractive mode must be done by an expert. On demand, Equisign team could assist on this task

- SAML Non Interractive - This plugin thus immediately redirects to the SAML IdP the user attempting to authenticate.

  For security reasons, SAML Configuration in Non Interractive mode must be done by an expert. On demand, Equisign team could assist on this task

- Simple SQL Database Contact Source - Configuring contact sources, as described in MFT Server Configuration Guide, enables an administrator to create a more complete contact list for the auto-complete function. Contact sources can be configured to use simple SQL databases and be attached to domains.

- LDAP Contact Source - Configuring contact as described in MFT Server Configuration Guide, enables an administrator to create a more complete contact list for the auto-complete function. Contact sources can be configured to use LDAP directories and be attached to domains. LDAP contact source configuration is not needed when user providers are configured.

6. Enter a parameter. The parameter must uniquely identify the plug-in instance. The parameter replaces the $0 variable in the field names for the configuration properties.
7. Click OK.
8. In the configuration fields, enter the required values using the tooltips available by mousing over the lightbulb icon.
9. Click Save Configuration.
10. When prompted, select Restart the application modules after configuration is reloaded to enable the plug-in.
11. Click Save and Reload Configuration.

4.3. Customize Login

An administrator with the System Setup right can control how the Managed File Transfer system authenticates a user by customizing the login process. Administrators can customize the login process by choosing the fields that are displayed in the login prompt. Most of the login parameters can be customized via the Login Customization page, but more advanced parameters are available on the general Advanced Settings menu. Login customization configurations will be saved as the default settings in the BASE configuration scope only. If a machine must have a separate customization, it must be configured on the Advanced Settings page.

Procedure 4.3. To configure customized login requirements:

1. Log in to the Managed File Transfer administration application as an administrator with the System Setup right.
2. Navigate to the Server Management | Setup | Login Customization page.
3. On the Login Customization page, configure the following authentication mechanism options:

   a. Require Domain Information - Select this option to require that a user's Managed File Transfer domain be identified before the user can log in. It is only a requirement to identify the Managed File Transfer domain of a user when a registered user corresponding to a single physical person belongs to more than one domain. Requiring the domain to be identified narrows the user lookup phase because users are only

searched in repositories related to the identified domain. In most cases, this option is not necessary. There are three ways to identify a user's domain:

- The user selects a domain from a list in the login page.
- The Managed File Transfer administration application identifies the user's domain by the HTTP parameter.
- The Managed File Transfer administration application identifies the user's domain by using the access URL to the Web server.

b. Domain Extraction Regex - This field will only be available if the Require Domain Information option is selected. If entered, the given regular expression is used to infer a user's Managed File Transfer domain from the URL used to access the application. For example, if the URL is `https://mft.opentrust.com/`, the regular expression could be `^http://([a-zA-Z0-1]+)\.opentrust\.com/.*$`. Leave the field empty if the Display List of Domains option is selected. Use the keyboard icon to test the regular expression before saving the settings.

c. Domain Mappings - This field will only be available if the Require Domain Information option is selected. Enter the mapping directions that will be used to map a domain name from the pattern extracted using the regular expression entered in the Domain Extraction Regex field. Refer to the corresponding help icon for configuration instructions. Leave this field empty if the Domain Extraction Regex option is left empty. The mapping expression will be determined where in "mft=MFT" mft is the domain identifier extracted from the URL and MFT is the domain application name. The Managed File Transfer administration application will attempt to determine the domain by the defined domain mapping in the following order:

   i. By matching the mapping defined in domain mappings if there is a match.

   ii. By matching a domain with the same name as the matched pattern.

   iii. By using the default mapping entry if there is one, such as "default=MFT".

d. Display List of Domains - This field will only be available if the Require Domain Information option is selected. Select this option to allow the user to explicitly identify their domain by selecting the domain they belong to from a displayed list at the login prompt. If this option is not selected, the Managed File Transfer domain that the user belongs to must be inferred from the Web server name. The rule to infer the domain name is defined in the domain mappings parameter.

e. Login Type - From the drop-down menu, choose the type of login prompt that will be displayed to the user when logging into the Managed File Transfer administration application:

   - Unified Login Prompt - The user will be prompted to enter both their login ID or email address and password at the same time.
   - Separate Identification and Authentication Phases - The user will first be prompted to enter the individual login ID or email address on an initial page, then will be directed to a second page to enter their password. By first identifying the user, the Managed File Transfer application is able to determine which authentication criteria the user must provide to access the application. For example, some users will need to provide a password while others might be asked to provide a one-time password. In most cases the identification and authentication phases do not need to be separated.

f. Identification Credentials - From the drop-down menu, select which elements the Managed File Transfer administration application will use to identify the user. Use the plus and minus icons to adjust the number of required credentials. "IDENT"

corresponds to the generic identifier term which will be displayed at the login prompt. When provided to the internal authentication scheme, the "IDENT" is used to search the user first by UID, then by email address.

g. Authentication Credentials - This field will only be necessary if Unified Login Prompt was selected as the login type. From the drop-down menu, select which elements the Managed File Transfer administration application will use to authenticate the user. Use the plus and minus icons to adjust the number of required credentials. In most cases, a single password is sufficient.

h. Authentication Schemes Order - Drag the authentication schemes and place them in the order that the Managed File Transfer administration application should use to try and authenticate a user. Users will be searched for and authenticated using only the selected authentication schemes. This step can be edited after additional authentication schemes are configured, as described in Section 4.2, “Configure Authentication or Contact Source Plug-ins”.

4. Click OK.

4.4. Configure Authentication Policies

Authentication policies enable an administrator to configure how users can be authenticated by the Managed File Transfer server application. An authentication policy can be Global to all Domains or Local to a single Domain. Authentication policies that are global to all domains are visible and available for use to all users within any domain. Authentication policies that are local to a domain are visible and available for use only to users within the domain selected during the configuration of the policy. Authentication policies that are global to all domains or local to a single domain can only be configured by an administrator with the Global Settings Management right. Authentication policies can be assigned to users, as described in Chapter 5, Manage Users.

Procedure 4.4. To configure an Authentication Policy:

1. Log in to the Managed File Transfer administration application as an administrator with the Settings Management right.

2. Navigate to the Settings | Policies | Authentication page.

3. On the Authentication page, choose to Create a New Authentication Policy or to Modify, Copy, or Remove an existing authentication policy.

4. If the choice was to create a new authentication policy, or to modify an existing authentication policy, on the create a new authentication policy page, configure the following authentication policy settings:

   a. Name and Description - Enter a name and description for the authentication policy. The name will be visible in other parts of the user interface for the administration application, for example, when selecting which authentication policy to use for a particular user. Providing detailed information in the name and description fields will make it easier to select the correct authentication policy in other parts of the user interface for the administration application.

   b. Scope - Choose the scope of the authentication policy by selecting Global or Local to a Domain. If local to a domain is selected, select a domain from the drop-down menu.

   c. Primary Authentication Scheme - From the drop-down menu, select an authentication scheme. The primary authentication scheme is used to authenticate the user in standard authentication mode.

d. Alternate Authentication Scheme - From the drop-down menu, select an authentication scheme. The alternate authentication scheme is used to authenticate the user when the alternate authentication mode is activated. Alternate authentication mode is an optional settings for user profiles. If it is not used, the alternate authentication scheme field can be left blank.

e. Password Policy - From the drop-down menu, select a password policy to apply to the authentication policy. This step is option. Select Minimal Validation if a unique password policy has not yet been configured, as described in Section 9.1.3, "Add/ Configure Password Policies", or if a password policy is not necessary. This option can be edited after all settings have been configured. This option will only be available if the internal authentication scheme relying on the internal Managed File Transfer user repository is selected as the primary or alternate authentication scheme.

   Note: OTP authentication plugins rely on the selected password policy to generate the OTP code.

f. If Default Authentication Scheme (internal) was selected as Primary or Alternate Authentication Scheme, set the following options:

   - Change password at first login - The label of this feature is somewhat misleading, because if this option is selected, the user is forced to change their password whenever an administrator reset it, not only upon the user account creation.

   - Allow Password Reset by User - Select this option to allow users to reset their own passwords by selecting a link on the end-user login page. If this option is not selected, the user will not have the option available on the end user application to reset their own password.

g. If OTP Authentication was selected as Primary or Alternate Authentication Scheme, set the following options:

   - SMS Sender - Enter the name of the sender. This name will be displayed to the end-user when he receives the text message.

   - SMS Body - Enter the content of the text message. Use the {0} variable to dynamically insert the OTP code in the content of the text message.

5. Click OK.

Chapter 5. Manage Users

Users of the Managed File Transfer application can be either administrators or end users. Users become administrators when they are given access control rights, otherwise they are end users whose capacity to exchange messages with others depends on the exchange policies they are given. A user is identified by the Managed File Transfer application with a UID, which may be a be the same value as an email address or an email and domain combination. Each user, throughout all domains, must have a different UID and email address unless the property auth.domain.forbidSameUserIdentificationInDifferentDomains has been deselected on the Advanced Settings page. If the Managed File Transfer configuration allows the creation of users with the same UID or email in different domains, then the authentication process should be configured so that the domain is provided during user authentication in order to unambiguously identify users. If the domain is not provided for users existing in more than one domain, those users will not be able to log in to the Managed File Transfer application. The User Management right enables administrators to create, edit, delete and search for users within one of their assigned domains. Because the User Management right is assigned per domain, new users can only be configured by an administrator that has the User Management right for the domain that the new user will be assigned to. Administrators with the User Management rights also have the ability to edit or delete users after they have been created. Tags, which can be created and attached to users as a means to help administrators refine user searches, can be created and edited by administrators with the global or local Settings Management right.

Note: Even if the option to forbid the same user identifications within different domains was unchecked on the Advanced Settings page (auth.domain.forbidSameUserIdentificationInDifferentDomains), the UID and email address for each user must be unique within a given domain.

In this chapter, administrators can:

- Section 5.1, “Create Tags”
- Section 5.2, “Add, Edit, and Delete Individual Registered Users”
- Section 5.3, “Add and Synchronize Registered Users By File Upload”

5.1. Create Tags

Tags are used to help further identify a user. Tags can be used as search terms when searching for a user in the user interface for the administration application. A tag can be assigned to multiple users to help identify users that have something in common. Tags are displayed in the end user application in user information tooltips and are available for selection when creating email templates. Tags can be created and assigned to users by administrators with the Settings Management right.

Procedure 5.1. To configure or edit a tag:

1. Log in to the Managed File Transfer administration application as an administrator with the Settings Management right.
2. Navigate to the User Management | Manage | Tags page.
3. On the Tags page, choose to Create a New Tag or to Modify or Remove an existing tag.
4. If the choice was to create a new tag or to modify an existing tag, on the create a new tag page, configure the following tag settings options:

a. Name and Description - Enter a name and description for the tag. The name of the tag will be displayed for selection in the user interface for the administration application and the end user interface.

b. Scope - Choose to make the tag available to all domains or available to a single domain by selecting Global or Local to a Domain. If local to a domain is selected, select a domain from the drop-down menu.

5. Click OK.

5.2. Add, Edit, and Delete Individual Registered Users

Administrators with the User Management right have the ability to add and manage a user's settings and their ability to send messages to other registered users as well as to guest users. The policies that control user privileges can be created by an administrator with the Settings Management right, as described in Chapter 9, Configure Settings.

Procedure 5.2. To add a new user or edit an existing user:

1. Log in to the Managed File Transfer administration application as an administrator with the User Management right in the domain that the user will be added to.
2. Navigate to the User Management | Manage | Users page.
3. On the Users page, use the search for users box to Modify or Remove an existing user, or select Create a New User and continue to Step 5.
4. If the choice is to modify or remove an existing user, use the search form on the User Management page to locate the user. An * may be used in all fields as a wildcard. To select or deselect multiple tags, use the Ctrl key during the selection or de-selection process. Select the user to be modified or deleted. Continue to the next step for more information on user settings.
5. On the Create a New User page, configure the following user settings:

   a. User ID - Enter a user ID for the user. By default, all alphanumeric characters are allowed as well as the special characters _, -, ., @ and :. The UID must match the User ID Regular Expression configured in the selected domain.

   b. Email - Enter an email address for the user.

   c. Domain - From the drop-down menu, select a domain for the user.

   d. First Name and Last Name - Enter the first and last name of the user.

   e. Language - Choose to use either the default language of the user's domain or choose Specific Language and select a language.

      Note: This language setting is used when displaying the Web application and when sending emails to the user. If the chosen language is not available for the web application, then the display language will depend on the browser's configuration and on the available languages. This language may be changed by the user when configuring preferences.

   f. Mobile Phone Number - Enter a valid phone number. If you enter a local phone number -for example 732 777 2924 if you live in the USA- ensure that its country matches with

the country set by the *client.defaults.phonenumber.region* property. If not, add the country code before your phone number -for example +1 732 757 2923.

g. Active - Select this option to enable the user to access the Managed File Transfer administration application. If Active is not selected, the user will not be able to authenticate and log in to the Managed File Transfer application. For example, this option can be used to temporarily deactivate a user account.

h. Expiration Date - To enable a date for the user account to expire, select Set Date and enter a date for the account to be deleted. An expiration date for the user account is not required. When an expiration date is set for a user account and the user account expires, the user account is marked as expired and the account is disabled during the grace period configured by the "batch.user.cleanup.grace" property, configurable on the Server Management | Setup | Advanced Settings page on the Base tab. After the grace period, the user account is deleted.

i. Authentication Policy - From the drop-down menu, select an authentication policy. The selected authentication policy will determine how the user can authenticate to the Managed File Transfer server during the login process. All authentication policies configured, as described in Section 4.4, “Configure Authentication Policies ”, will be available in the drop-down menu.

j. Password - Enter and confirm the password the user will use during authentication, or select to generate a random password. A password will only be required if the selected authentication policy included the "Default Authentication Scheme" based on the internal Managed File Transfer user repository where the password is stored. If there is a password policy selected for the authentication policy, the user's password must respect the selected password policy. The link Generate random password allow auto generating a random password according to the password policy.

k. User Quota Policy - From the drop-down menu, select a user quota policy. This field is only available if user quota are enabled for the domain selected for the user.

l. Exchange Policy - From the drop-down menu, select an exchange policy. The exchange policy control to whom the user will be allowed to exchange messages. If exchange policies have not yet been configured, select None. This option can be edited after exchange policies have been configured, as described in Section 9.2.2, “Create an Exchange Policy”. Until an exchange policy is selected, the user will not have the ability to send messages except for within projects created by other users.

m. Tags - From the drop-down menu, select tags to apply to the user. To attach multiple tags, use the add and subtract icons. If tags have not yet been configured, this step can be edited after tags are configured, as described in Section 5.1, “Create Tags”.

n. Allow sending messages using the File Connector - If this option is selected, the user will have access to send messages through web services using the SOAP and REST protocol.

6. Click OK to save a new user or to modify an existing user's settings. Click Delete to delete an existing user.

   Note: Deleting a user will also delete all messages sent by that user, but will not remove projects created by the user. Projects can only be removed by the user that created the project.

5.3. Add and Synchronize Registered Users By File Upload

Administrators with the User Management right have the ability to import and update registered users by uploading a `.csv` or a `.json` file. The uploaded file is associated with a user provider, which must be configured, as described in Section 9.4.1, “Configure User Providers”, before the file can be uploaded. Examples of the required `.csv` and `.json` file formats are provided for download in the UI. When uploaded, the file serves as a short-lived source repository for the synchronization process of registered users, in the same way an LDAP directory would server as the source repository for users imported via LDAP. Both file upload and LDAP directory source repositories make use of datasource configurations, with one pre-configured and unmodifiable datasource named File Import serving as the datasource for all uploaded files used to add and synchronize registered users.

During synchronization, registered users linked to the user provider selected for the file upload and entered in the uploaded file are updated, registered users linked to the user provider selected for the file upload and not entered in the uploaded file are deleted, and user entries contained in the uploaded file but not yet associated with a user provider are added as registered users. The uploaded file is deleted immediately following the synchronization process.

Administrators can also use a REST Connector to supply the synchronization file, as described in the MFT Connectors Developer Guide, instead of using the UI as described in this section.

Procedure 5.3. To add or update registered users via file upload:

1. Log in to the Managed File Transfer administration application as an administrator with the User Management right for the domain(s) that the users will be imported to.
2. Navigate to the User Management | Synchronize | Users page.
3. On the User Synchronization page, select a user provider. All user providers that have been configured with "File Import" selected as the datasource will be available for selection.
4. In the Data File field, enter or browse to and select the directory path and file name of the file containing new or edited users.
5. Click Upload Now.
6. On the User Synchronization Preview pop-up, review the actions that will be performed during the synchronization and click Launch Synchronization.
7. Review the provided synchronization summary and correct any errors.

Chapter 6. Manage Rights

The Access Control section of the Managed File Transfer administration application enables administrators to assign and manage the rights of individual users or groups of users. Administrators can use the access control configurations to create high-level administrators during the initial setup process and lower-level administrators as needed. The Access Control settings also enable administrators to create and manage groups. Groups can be used to assign the same rights to more than one user at a time.

6.1. Configure Groups

Groups can be created and edited by an administrator with the Group Management right. Groups are useful when configuring the same rights for several users, such as a group of low-level administrators that all need identical access or users in the same business unit. Configuring rights for a group rather than each individual user is more efficient and allows administrators to be accurate in assigning rights.

A group may have members, managers, and impersonators. Group members share the rights of the group. Group managers can manage the group members by adding or removing them. Group impersonators can act on behalf of any group member. Group managers and impersonators must be explicitly granted their rights and grant ability in the group configuration.

Administrators with the Impersonation and Group Management rights can configure impersonation at the group level: add and remove groups and users with the ability to impersonate members of the group as well as configure impersonators' abilities to grant the group-level Impersonation right to other groups and users.

Impersonation can be configured when using the MFT File Connector with an external application that will send messages on behalf of MFT users. Refer to the MFT Connectors Developer Guide for additional information on the MFT File Connector. Impersonation can also be configured for use with the MFT SMTP Connector to impersonate MFT users when redirecting emails from an organization's email system, such as Microsoft Exchange, to MFT. Organizations might want to use the MFT SMTP Connector and the Impersonation right for emails with large attachments, for example.

This section describes how to configure impersonation at the group level when only group members will be impersonated. When impersonation will be used for all MFT users, the system-wide Impersonation right should be used, as described in Section 6.2, “Configure Rights”.

Procedure 6.1. To configure a group:

1. Log in to the Managed File Transfer administration application as an administrator with the Group Management right. To configure impersonation, administrators must also have the Impersonation right. To manage users within groups, such as when adding individual users as members or impersonators, administrators must also have the User Management right. Certain functionalities in the interface will only be available if the administrator has the appropriate right. If the functionality for a particular tab is not available, continue to the steps for the next tab.
2. Navigate to the Access Control | Management | Groups page.
3. On the Groups Management page, choose to Create a New Group or to Modify or Remove an existing group.
4. If the choice was to create a new group or to modify an existing group, on the create/edit a new group page, on the General tab, enter a Name and Description for the group.

The name and description will be visible in other parts of the user interface for the administration application, for example, when selecting which group to edit. Providing detailed information in the name and description fields will make it easier to select the correct group in other parts of the user interface.

5. Click OK.
6. On the Managers tab, select Add New Group Managers.
7. In the Add New Group Managers window, enter any known information into the search criteria box to search for users or groups. An * may be used in all fields as a wildcard. Click OK. All configured groups and all users in a domain for which the administrator has the User Management right can be returned in the search results.
8. Select the user(s) or group(s) who should have the ability to add or remove members from the group and click Select. Then select the checkbox in the Execute column for each user or group that should have the ability to add or remove members of the group. Then decide whether each user or group with the ability to add and remove users should be able to grant the right to add and remove users to other users and groups and configure the level of grant ability for the users or groups. To grant the user or group the ability to grant the right to other users or groups, select Execute in the Grant Ability column. To grant the user or group the ability to grant the right to other users and groups and give other users and groups the right to grant the right to others, select Execute & Grant to Others in the Grant Ability column.
9. Click OK.
10. On the Impersonators tab, select Add New Group Impersonators.
11. In the Add New Group Impersonators window, enter any known information into the search criteria box to search for users or groups. An * may be used in all fields as a wildcard. Click OK. All configured groups and all users in a domain for which the administrator has the User Management right can be returned in the search results.
12. Select the user(s) or group(s) who should have the ability to impersonate members of the group and click Select. Then select the checkbox in the Execute column for each user or group that should have the ability to impersonate members of the group. Then decide whether each impersonator should be able to grant the right to impersonate to other users and groups and configure the level of grant ability for the impersonator. To grant the user or group the ability to grant the right to other users or groups, select Execute in the Grant Ability column. To grant the user or group the ability to grant the right to other users and groups and give other users and groups the right to grant the right to others, select Execute & Grant to Others in the Grant Ability column.
13. Click OK.
14. On the Members tab, select Add New Group Members.
15. In the Add New Group Members window, enter any known information into the search criteria box to search for users or groups. An * may be used in all fields as a wildcard. Click OK.
16. Select the user(s) or group(s) to add to the group and click Select.
17. Click OK.

6.2. Configure Rights

Administrators with the User Management right have the ability to configure and edit the rights of an individual user or a group of users within domains assigned to the administrator.

Procedure 6.2. To configure or edit the rights of a user or group:

1. Log in to the Managed File Transfer administration application as an administrator with the User Management right with rights to Execute and Grant to Others configured for the domain that the user or group is in.
2. Navigate to the Access Control | Management | Rights page.
3. On the Rights Management page, enter any known information into the Search for Users or Search for Groups box. To search for all users, enter the wildcard * into any search parameter field.
4. Click OK.
5. Select from the search results list the user or group whose rights need to be configured or modified.
6. On the Edit Rights of User or Group page, on the Group Membership tab, select a group that the user or group should be added to. This option should only be selected if it is appropriate to assign all the rights of the selected group to the user or group whose rights are being configured.
7. On the Global Rights tab, in the row for each right:
   - To grant the user or group the right, select the checkbox in the Execute column.
   - To grant the user or group the ability to grant the right to other users or groups, in the drop-down menu select Execute.
   - To grant the user or group the ability to grant the right to other users and groups and give others the right to grant the right to others, in the drop-down menu, select Execute & Grant to Others.
8. Click OK.
9. On the Rights Limited by Domain tab, in the row for each right:
   - To grant the user or group the right, select the checkbox in the Execute column.
   - To grant the user or group the ability to grant the right to other users or groups, in the drop-down menu select Execute.
   - To grant the user or group the ability to grant the right to other users and groups and give others the right to grant the right to others, in the drop-down menu, select Execute & Grant to Others.
10. Click OK.

Chapter 7. Configure PDF Document Signing

The MFT PDF document signing feature allows documents sent by users to be signed by the MFT application. It is important to note that PDF documents are signed server-side using a server-configured private key, not client-side using a user's private key. Administrators can configure PDF signature policies that can then be attached to a sending policy in order to control how registered users and guest users are able to access the document signing feature. Before a PDF signature policy can be configured, at least one trusted keypair must be configured. If the signature policy is configured to require the inclusion of the certificate authorities (CAs) that issued the signer certificate within the signature, then trusted certificates for those CAs must be configured.

According to the configured PDF signature policy, the PDF signatures generated may be visible or not; if visible, their graphical appearance can be configured (position, text displayed, etc.)

In this section, administrators can:

- Section 7.1, “Manage Trusted Certificates for Signing”
- Section 7.2, “Configure Keypairs”
- Section 7.3, “Add/Configure PDF Signature Policies ”

7.1. Manage Trusted Certificates for Signing

If a signature policy requires the inclusion of CA certificates or CA CRLs in the signature, trusted certificates for these CAs must be added to the Managed File Transfer administration application. The trusted certificates are used to compose the certificate chains used to sign PDF documents. Administrators should be familiar with the principle concepts of PKIs, CAs, and CRLs before attempting to manage trusted certificates.

Each trusted certificate must be unique; multiple trusted certificates cannot be created using the same CA certificate. If a signature policy requires CA certificates, the entire CA certificate chain must be trusted, including the root CA, by configuring trusted certificates for each certificate in the chain.

Procedure 7.1. To configure a trusted certificate:

1. Log in to the Managed File Transfer administration application as an administrator with the Keypairs Management right.
2. Navigate to the Server Management | Certificates and Keys | Trusted Certificates page.
3. On the Trusted Certificates page, choose to Add a New Trusted Certificate or to Modify or Remove an existing trusted certificate.
4. If the choice was to configure a new trusted certificate, on the Add a New Trusted Certificate page, enter a Name and Description for the trusted certificate. The name will be visible in other parts of the administration application interface, for example, when selecting a trusted certificate for use in a signature policy. Providing detailed information in the name and description fields will make it easier to select the correct trusted certificate in other parts of the administration application interface.
5. Click Import Certificate.

6. On the Import Certificate pop-up, select a method for importing the trusted certificates and enter the required information:

   - Upload from Local File - If the file containing the CA's certificate has been copied to a local directory on the same machine as the browser being used to access the Managed File Transfer administration application, browse to and select the directory path and file name of the file containing the CA certificate.

   - Retrieve from URL - Cut and paste the URL of the CA certificate if available on a PKI Web page.

     By default, the URL must be in `http` format. To use a URL in `https` format: the CA that issued the certificate for the Web server from which the CRL will be downloaded must be added to the `/opt/opentrust/mft/var/mnt/secure/truststore.jks` file using "keytool", `https` certificate downloads will only be successful if the data in `truststore.jks` is valid, and Tomcat must be restarted each time `truststore.jks` is updated.

   - Paste PEM Format - In the Certificate in PEM field, paste the full PEM format of the certificate to upload.

7. Click Import Certificate.

8. Configure the CRL download URL and click Test. This is the URL of the CRL produced by the CA, not to be confused with the CRL validating the CA, produced by the CA's parent. The download URL can be changed if the CA is moved to a new server or host location. The URL must be in `http` format.

9. To use the HTTP proxy defined on the Server Management | Setup | Advanced Settings page in the `proxy.host` field, select Use Proxy.

10. Click OK.

7.2. Configure Keypairs

Before a PDF signature policy can be configured, a keypair that can be used to generate server-side digital signatures must be configured. A keypair is composed of a private key and a certificate that can be used to generate server-side digital signatures. The keypair can be stored locally on the Managed File Transfer server application or on an external cryptographic device known as an HSM. If a keypair will be stored on an HSM, the HSM client software must be installed on each end user application server before a keypair can be configured.

For security reasons, HSM Configuration in Non Interractive mode must be done by an expert. On demand, Equisign team could assist on this task

Procedure 7.2. To configure a keypair:

1. Log in to the Managed File Transfer administration application as an administrator with the Keypairs Management right.

2. Navigate to the Server Management | Certificates and Keys | Keypairs page.

3. On the Keypairs page, choose to Add a New Keypair or to Modify or Remove an existing keypair.

4. If the choice was to create a new keypair, on the create a new keypair page, enter a Name and Description for the keypair. The name will be visible in other parts of the administration

application interface, for example, when selecting which keypair to use for a PDF signature policy. Providing detailed information in the name and description fields will make it easier to select the correct signer in other parts of the administration application interface.

5. Select a private key type:

   - Software - Select this option to have the private key and certificate extracted from an imported PKCS#12 file and stored in an internal repository of the Managed File Transfer server application.
   - Hardware - Select this option if the private key is available in a Hardware Security Module (HSM). This is the most secure storage medium.

6. If the software option was selected: in the Import PKCS12 box, configure the required fields:

   a. Click Import PKCS#12 File.

   b. On the Import PKCS#12 pop-up, for the Select PKCS#12 File field, browse to or enter the file path location for the PKCS#12 file.

   c. In the PKCS#12 Password field, enter the password associated with the PKCS#12 file.

   d. Click Import PKCS#12.

   e. To test the PKCS#12's ability to generate a digital signature, click Test Signature.

   f. Close the success message.

7. If an HSM was selected for the private key type, complete the configuration fields for the HSM in consultation with an assigned Equisign technical representative or refer to the tooltips in the administration interface for more information.

8. To save the configuration, click OK.

9. If the Hardware option was selected, configure the following required fields:

   a. HSM PKCS#11 Library Path - In the text-entry field, enter the PKCS#11 library path.

   b. HSM Slot ID - Using the up and down arrows, configure the value for the slot ID.

   c. HSM Certificate Label - In the text-entry field, enter the certificate label.

   d. HSM PKCS#11 Options - In the text-entry field, enter the PKCS#11 options. To enter multiple options, separate each option with a carriage return.

   e. HSM Password - Enter and confirm the password associated with the HSM.

7.3. Add/Configure PDF Signature Policies

PDF signature policies can be used to configure how and when a PDF signature is needed and used. After configuration, PDF signature policies can be applied to sending policies, as described in Section 9.1.4, “Add/Configure Sending Policies”.

Procedure 7.3. To configure a PDF signature policy:

1. Log in to the Managed File Transfer administration application as an administrator with the Settings Management right.

2. Navigate to the Settings | Policies | Signature page.

3. On the PDF Signature Policies page, choose to Create a New PDF Signature Policy or to Modify, Copy, or Remove an existing PDF signature policy.

4. If the choice is to create a new PDF signature policy or to modify an existing PDF signature policy, on the Configure PDF Signature Policy page, configure the following PDF signature policy options:

    a. Name, Title, and Description - Enter a name, title, and description for the PDF signature policy. The name will be visible in other parts of the administration application interface, for example, when selecting which PDF signature policy to use for a sending policy. Providing detailed information in the name and description fields will make it easier to select the correct PDF signature policy in other parts of the administration application interface.

    b. Scope - Choose to make the PDF signature policy available to all domains or available to a single domain by selecting Global or Local to a Domain. If Local to a Domain is selected, select a domain from the drop-down menu.

    c. Signer - From the drop-down menu, select the signer. The signer is the keypair that this policy will use to sign documents. All keypairs configured as described in Section 7.2, “Configure Keypairs” will be available for selection. If the signer certificate is expired, signature will fail

    d. Document Digest - From the drop-down menu, select a document digest. The document digest is the algorithm used to compute the digest of the PDF document when it is signed.

    e. Include CA Chain - Select this option to include the signer's CA chain in the PDF signature. If selected, the entire CA chain of the trusted certificate will be included in the signature. Before selecting this option make sure that the entire CA chain, including the root CA, has been configured as described in Section 7.1, “Manage Trusted Certificates for Signing” and that there are no expired CA certificates within the chain. If one of those conditions is not met, signature will fail.

    f. Include CRL - From the drop-down menu, choose one of the CRL options:

        - No - No CRL will be included in the PDF signature.

        - Signer's CRL Only - Only the CRL of the CA that issued the Signer certificate will be included.

        - Whole CRL Chain - The CRL issued by each CA in the Signer certificate chain, including the root CA, will be included.

        If one or more CRLs are included in the signature, the CRL check is always implicitly performed at signing time. CRLs may be extensive, so including CRLs in the signature could significantly increase the size of the PDF document. Before selecting this option, make sure that the entire CA chain, including the root CA, has been configured as described in Section 7.1, “Manage Trusted Certificates for Signing”, that there are no expired CA certificates within in chain, and that each CA CRL is up to date. If one of those conditions is not met, signature will fail.

    g. Check CRL - This option is not available if the CRL chain is included in the signature (see above), because the CRL check is then implicitly performed. From the drop-down menu, choose which CRL to check during the signing:

        - Signer's CRL Only - Only the Signer certificate's revocation status will be checked.

        - Whole CRL Chain - The revocation status of each CA of the Signer certificate chain will be checked.

Before selecting this option, make sure that the entire CA chain, including the root CA, has been configured as described in Section 7.1, “Manage Trusted Certificates for Signing”, that there are no expired CA certificates in the chain, and that each CA CRL is up to date. If one of those conditions is not met, signature will fail.

h. Finalize Signature - Select this option to enforce the rule that a document can only be signed once. An attempt to sign the same document twice will not be rejected when the message is sent, but the second signature would appear invalid using Adobe Reader. If this option is selected, a stamp icon will be displayed next to the signature properties viewed using Adobe Reader.

i. Signed File Maximum Size - Using the up and down arrows, configure the maximum size for files that should be signed. Any file sent in a context where this policy applies and whose size exceeds this configured value will be rejected.

j. Reason - In the text-entry field, enter the reason for the PDF signature. The value of this field is displayed in the "Signature Properties" panel of Adobe Reader.

k. Location - In the text-entry field, enter the location where the PDF signature was signed. The value of this field is displayed in the "Signature Properties" panel of Adobe Reader.

l. Contact - In the text-entry field, enter the contact information for the PDF signature. An email address is suggested. The value of this field is displayed in the "Signature Properties" panel of Adobe Reader.

m. Signature Name - In the text-entry field, enter the name for the PDF signature. The name is the internal name of the PDF field containing the signature data created in the PDF document when signing. If no value is provided a name will be automatically generated when signing.

n. Add a Timestamp - Select this option to add a timestamp issued by a time stamping authority (TSA) to the PDF signature. If selected, configure the following timestamp options:

    i. Timestamp Server URL - In the text-entry field, enter the URL of the timestamp server. If the EquiSign Time Stamping Authority (TSA) product is used, enter the URL in the following format: `http://server/TSS/HttpTspServer`.

    ii. Use Proxy - Select this option to use the HTTP proxy defined on the Server Management | Setup | Advanced Settings page in the `proxy.host` field when connecting to a timestamp server.

    iii. Timestamp Digest - From the drop-down menu, select the digest algorithm applied to the signature before submitting it to the Time Stamping Authority.

    iv. Timestamp Policy OID - In the text-entry field, enter the policy that the Time Stamping Authority ("TSA") is expected to use for creating the time stamp token. Use the dotted OID notation. If no policy is requested, the TSA will use its own default policy.

o. Add a Visible Signature - Select this option to add a graphical visible signature on top of a single page in the PDF document. This signature may contain some text and a background image and will be applied to all documents signed using this policy. Adding a new page to a previously signed PDF document will invalidate all the previous signatures. Select this option only if you are sure the documents that will be signed have never been signed before being uploaded with the Managed File Transfer application. If selected, configure the following signature options:

i. Signature Page - From the drop-down menu, select the page on which the visible signature will be displayed. Adding a new page to a previously signed PDF document will invalidate the first signature; select this option only if you are sure the document will be signed only once.

ii. Text - In the text-entry field, enter the text that will appear in the signature. The text may contain the following variables that will be dynamically replaced when the signature occurs:

- [SIGNING_TIME] - Enter this text for the signing time using the "yyyy-MM-dd" and "HH:mm:ss" date format and UTC timezone to be displayed.
- [SIGNER_DN] - Enter this text for the signer certificate subject DN to be displayed.
- [SIGNER_NAME] - Enter this text for the signer certificate subject CN value to be displayed. If the signer certificate has no CN attribute, the whole subject DN will be displayed.
- [USER_ID] - Enter this text for the identifier of the current user in session to be displayed. For a registered user, the login UID will be displayed. For a guest user, the email address will be displayed.
- [USER_EMAIL] - Enter this text for the email address of the current user in session to be displayed. This applies to both registered and guest user.
- [USER_NAME] - Enter this text for the first-name and last name of the current registered user in session to be displayed. For a registered user, the user's first name and last name will be displayed. For a guest user, the user's email address will be displayed.
- [USER_SHORTNAME] - Enter this text for a shortened version of the name of the current user in session to be displayed. For a registered user, the first character of the user's first name and their last name will be displayed. For example, `J. Smith`. For a guest user, the user's email address will be displayed.
- [USER_INITIALS] - Enter this text for the initials of the current user in session to be displayed. For a registered user, the first character of the user's first name and the first character of the user's last name will be displayed. For example, `J.S.`. For a guest user, the user's email address will be displayed.
- [BR] - Enter this text to start a new line.

iii. Font Family - From the drop-down menu, select the font that the signature text will be displayed in.

iv. Font Style - From the drop-down menu, select the font style that the signature text will be displayed in.

v. Font Size - Use the up and down arrows, or enter in the text-entry field, the font size that the signature text will be displayed in.

vi. Font Color - Click on the color box, and click to select the font color that the signature text will be displayed in.

vii. Background Image - Click Upload Image to select an image to be displayed as the background image of the signature. Click No Image to only include text in the signature.

viii. Position on Page - Click on a circle to select the position of the page that the signature will be located in.

p. Add a Watermark Signature - Select this option to add a graphical visible watermark on top of all the pages in the PDF document. This watermark may contain some text and a background image and will be applied to all documents signed using this policy. Adding a watermark to a previously signed PDF document will invalidate all the previous signatures. Select this option only if you are sure the documents that will be signed have never been signed before being uploaded with the Managed File Transfer application. If selected, configure the following watermark options:

   i. Text - In the text-entry field, enter the text that will appear in the watermark. The text may contain the following variables that will be dynamically replaced when the watermark occurs:

      - [SIGNING_TIME] - Enter this text for the signing time using the "yyyy-MM-dd" and "HH:mm:ss" date format and UTC timezone to be displayed.

      - [SIGNER_DN] - Enter this text for the signer certificate subject DN to be displayed.

      - [SIGNER_NAME] - Enter this text for the signer certificate subject CN value to be displayed. If the signer certificate has no CN attribute, the whole subject DN will be displayed.

      - [USER_ID] - Enter this text for the identifier of the current user in session to be displayed. For a registered user, the login UID will be displayed. For a guest user, the email address will be displayed.

      - [USER_EMAIL] - Enter this text for the email address of the current user in session to be displayed. This applies to both registered and guest user.

      - [USER_NAME] - Enter this text for the first-name and last name of the current registered user in session to be displayed. For a registered user, the user's first name and last name will be displayed. For a guest user, the user's email address will be displayed.

      - [USER_SHORTNAME] - Enter this text for a shortened version of the name of the current user in session to be displayed. For a registered user, the first character of the user's first name and their last name will be displayed. For example, `J. Smith`. For a guest user, the user's email address will be displayed.

      - [USER_INITIALS] - Enter this text for the initials of the current user in session to be displayed. For a registered user, the first character of the user's first name and the first character of the user's last name will be displayed. For example, `J.S.`. For a guest user, the user's email address will be displayed.

   ii. Font Family - From the drop-down menu, select the font that the watermark text will be displayed in.

   iii. Font Style - From the drop-down menu, select the font style that the watermark text will be displayed in.

   iv. Font Size - Use the up and down arrows, or enter in the text-entry field, the font size that the watermark text will be displayed in.

   v. Font Color - Click on the color box, and click to select the font color that the watermark text will be displayed in.

vi. Background Image - Click Upload Image to select an image to be displayed as the background image of the watermark. Click No Image to only include text in the watermark.

vii. Position on Page - Click on a circle to select the position of the page that the watermark will be located in.

5. Click OK.

Chapter 8. Configure At-rest Encryption

When the at-rest encryption feature is enabled, all files sent through MFT are encrypted when the sender uploads them, and decrypted when the receiver downloads them. This is done server-side with administrator-defined keys, so the encryption and decryption process is completely transparent to the sender and to the receivers. This prevents data loss if an attacker manages to access the NAS where the files are stored.

Encryption keys are stored in the DB, either unencrypted or encrypted ("wrapped") by a key stored on a HSM. In the latter case, all key wrapping operations are done on the HSM, which means the wrapping key never leaves the HSM. In the event of a security breach administrators can disable the HSM to prevent attackers from unwrapping the key, rendering the stored files useless.

8.1. Manage KeyPairs for at-rest encryption

At-rest encryption settings are applied system-wide, i.e. they are not declined in various policies attached to domains.

Procedure 8.1. To enable at-rest encryption:

1. Log in to the Managed File Transfer administration application as an administrator with the Keypairs Management right.
2. Navigate to the Server Management | Certificates and Keys | At-rest encryption page.
3. On the At-rest encryption page, choose to Create a New secret key.
4. Define a name for the new secret key.
5. Choose a key type:
   - Software: the key will be stored unencrypted in the database.
   - Hardware: the key will be encrypted (wrapped) by another key stored in the HSM, before being stored in the database.
6. Configure the key:
   - Software:
     - Secret key: the passphrase from which the encryption key will be derived. The passphrase can either be defined manually or randomly generated by MFT.
   - Hardware: configure the HSM as described in the Configure Signature chapter.
7. Click the "OK" button to save the new secret key and go back to the main screen.
8. Enable the key:
   a. In the Active secret key dropdown menu, select the newly created key.
   b. Define the Cache retention duration: if this value is set at 1 or higher, the (unwrapped) key will be kept in memory for this amount of minutes before being fetched from the database (and unwrapped in the case of a Hardware key) again. This option is mostly

used to control how often the HSM will be called to unwrap the key. If this option is set at 0 or -1, caching is disabled and the key will be fetched from the database (and unwrapped in the case of a Hardware key) every time a file needs to be encrypted or decrypted.

Keys can be added and activated as often as needed with no impact on files encrypted with previous keys. As long as the previous key is present in the secret key list, the files will be available for download. To prevent these files from being decrypted, the key must be deleted by clicking on the recycling bin icon.

For security reasons, HSM Configuration must be done by an expert. On demand, Equisign team could assist on this task

Chapter 9. Configure Settings

Settings options allow administrators to customize the ways that users interact with the Managed File Transfer application. Specifically, settings allow administrators to customize the functionality of domains by creating themes or an information message as well as configuring how users interact with each other through policies. Most policies can be defined as either domain policies or user policies. Domain policies add functional capabilities to the application, whereas user policies control the access abilities that users have within the Managed File Transfer application. Domain policies are designed to give administrators the ability to maintain administrative and technical features associated with domains. User policies enable administrators to customize the access that individual users have to the Managed File Transfer application. In addition to policies, there are setting options that are designed to further customize domains. These settings are optional, but give administrators more customization options for domain. Policy settings can be available to all domains or available to a single domain by configuring the scope as global or local to a domain. Global policy settings are the options that are configured by an administrator with global rights to be available and applicable to any user within any domain. Local policy settings can be applied only to users within the domain they are configured for by an administrator with the local rights to that specific domain. If there is only one domain or if all policy settings should be available for use to all domains, only global policies will need to be configured.

In this chapter, administrators can:

- Section 9.1, “Configure Domain Policies”
- Section 9.2, “Configure Exchange Settings”
- Section 9.3, “Create/Upload Themes”
- Section 9.4, “Configure Repositories”
- Section 9.5, “Configure Additional Settings”

9.1. Configure Domain Policies

Domain Policy settings enable administrators to create rules and guidelines for how users within a specific domain interact with the Managed File Transfer application. After a domain policy is configured, it can be applied to the appropriate domain by an administrator with the Domain Management right by editing the domain, as described in Chapter 3, Configure Domains.
The scope of domain policies can be configured as either Global to all Domains or Local to a Domain. Domain policies that are global to all domains will be visible and available for use to all domains and can only be configured by an administrator with the Global Settings Management right. Local domain policies will only be visible and available for use to the domain selected during configuration of the domain policy and can only be configured by an administrator with the Local Settings Management right for the selected domain or with the Global Settings Management right.

In this section, administrators can:

- Section 9.1.1, “Add/Configure User Quota Policies”
- Section 9.1.2, “Add/Configure File Filtering Policies”
- Section 9.1.3, “Add/Configure Password Policies”
- Section 9.1.4, “Add/Configure Sending Policies”
- Section 9.1.5, “Configure Pre-Archiving”

9.1.1. Add/Configure User Quota Policies

Quota policies are used to set a maximum amount of storage space for the users of a domain. Administrators can set a domain-wide quota with a numeric value when configuring a domain, as described in Chapter 3, Configure Domains. Domain-wide quotas set a limit for the total, combined storage space for all users belonging to a domain. To set quotas for individual users of a domain, an administrator with the Settings Management right must configure a quota policy. Administrators with the User Management right can apply a quota policy to an individual user, as described in Chapter 5, Manage Users.

Procedure 9.1. To configure a quota policy:

1. Log in to the Managed File Transfer administration application as an administrator with the Settings Management right.
2. Navigate to the Settings | Policies | User Quota page.
3. On the Quotas page, choose to Create a New Quota Policy or to Modify, Copy, or Remove an existing quota policy.
4. If the choice was to create a new quota policy or to modify an existing quota policy, on the create a new quota policy page, configure the following quota policy settings:
    a. Name and Description - Enter a name and description for the quota policy. The name will be visible in other parts of the user interface for the administration application, for example, when selecting which quota policy to use for a particular user. Providing detailed information in the name and description fields will make it easier to select the correct quota policy in other parts of the user interface for the administration application.
    b. Scope - Choose to make the quota policy available to all domains or available to a single domain by selecting Global or Local to a Domain. If local to a domain is selected, select a domain from the drop-down menu.
    c. Activate User Quota - Select this option to activate the user quota. If selected, configure the general quota options:
        i. Maximum Storage Usage - Enter a value or use the up and down arrows to set the maximum storage usage for the user.
        ii. Warning Threshold - Enter a value or use the up and down arrows to set percentage of the maximum storage space that can be reached before a notification warning message is sent to the user.
    d. Activate Maximum Message Size Limit - Select this option to activate a maximum message size limit for the user. If selected, configure the limitation on message size option:
        - Maximum Message Size - Enter a value or use the up and down arrows to set the maximum message size for the user.
5. Click OK.

9.1.2. Add/Configure File Filtering Policies

File Filtering policies enable administrators to control which types of files can be either accepted or rejected. Administrators can create a policy that blocks a list of specified file types or only allows a list of specified file types. For more detailed information, refer to the help icons in the user interface for the administration application.

Procedure 9.2. To configure a file filtering policy:

1. Log in to the Managed File Transfer administration application as an administrator with the Settings Management right.
2. Navigate to the Settings | Policies | File Filtering page.
3. On the File Filtering Policies page, choose to Create a New File Filtering Policy or to Modify, Copy, or Remove an existing file filtering policy.
4. If the choice was to create a new file filtering policy or to modify an existing file filtering policy, on the create a new file filtering policy page, configure the following file filtering policy options:
    a. Name and Description - Enter a name and description for the file filtering policy. The name will be visible in other parts of the user interface for the administration application, for example, when selecting which file filtering policy to use for a sending policy. Providing detailed information in the name and description fields will make it easier to select the correct file filtering policy in other parts of the user interface for the administration application.
    b. Scope - Choose to make the file filtering policy available to all domains or available to a single domain by selecting Global or Local to a Domain. If local to a domain is selected, select a domain from the drop-down menu.
    c. Filtering Type - Select to create either a black list or white list. Selecting a black list filtering type enables the administrator to identify the specific file types to be blocked, while choosing a white list enables the administrator to identify the specific files to be allowed. A white list filtering type is highly recommended.
    d. Archive Files Management - From the drop-down menu, select the recursion level at which archive files should be allowed. It can be selected to forbid all archive type files, or to attempt to inspect the contents of the files recursively, but only up to two recursion levels. Since using archive containers is the most obvious way to circumvent a file filtering policy, it is recommended to be as restrictive as possible.
    e. Preset Filters - From the drop-down menu, select the type of file to be added to the black or white list filter. Use the plus and minus icons to adjust the amount of file types on the list.
5. To manually configure a file type to be added to the black or white list filter, click Advanced and refer to the instructions in the help icons in the user interface for the administration application.

    Click OK.

9.1.3. Add/Configure Password Policies

Passwords can be used to authenticate users as they attempt to log in to the Managed File Transfer administration application if the authentication scheme selected for their domain uses the Managed File Transfer registered-user repository. Passwords are also used when encryption of files is enabled within a sending policy because the encryption algorithm is based on passwords typed by users when they send an encrypted file, as described in Section 9.1.4, “Add/Configure Sending Policies”. A password policy can be configured to set guidelines for the type and quality of password a user is able to provide.

The Managed File Transfer server application is installed with a default password policy that is used if administrators do not configure and apply other password policies; the default name for the default password policy is the "Simple Password Policy." To view the password requirements

imposed by the default password policy, navigate to the Settings | Policies | Password page, open the default password policy, and view the configured options.

Procedure 9.3. To configure a password policy:

1. Log in to the Managed File Transfer administration application as an administrator with the Settings Management right.
2. Navigate to the Settings | Policies | Password page.
3. On the Password Policies page, choose to Create a New Password Policy or to Modify, Copy, or Remove an existing password policy.
4. If the choice was to create a new password policy or to modify an existing password policy, on the create a new password policy page, configure the following password policy options:
    a. Name, Title, and Description - Enter a name, title, and description for the password policy. The name will be visible in other parts of the user interface for the administration application, for example, when selecting which password policy to use for an authentication policy or sending policy. Providing detailed information in the name and description fields will make it easier to select the correct password policy in other parts of the user interface for the administration application. The title will be visible to the users of the domain that the password policy is applied to. When giving the password policy a title, select all of the languages used by users in the domain for which the password policy is configured for.
    b. Scope - Choose to make the password policy available to all domains or available to a single domain by selecting Global or Local to a Domain. If local to a domain is selected, select a domain from the drop-down menu.
    c. Minimum Length - Enter a value or use the up and down arrows to set the minimum number of characters required in the password.
    d. Maximum Length - Enter a value or use the up and down arrows to set the maximum number of characters allowed in the password.
    e. Minimum Number of Unique Characters - Enter a value or use the up and down arrows to set the number of unique characters required in the password. For example, if the maximum length is four characters and the minimum number of unique characters is four, then each of the four numbers or letters in the password must be unique, such as `1234` or `ABCD`. Another example would be a password with a maximum length of seven characters and a minimum of four unique characters, where `1122334` would be a valid password.
    f. Forbidden Passwords - Forbid specific password choices, such as `1234` or `MYPASSWORD`. multiple password entries must be separated by a carriage return, for example:

        ```
        1234
        MYPASSWORD
        ```

    g. Forbid Sequences - Forbid successive number and letter sequences. Includes both ascending and descending sequences, such as `1234`, `9876`, `ABCD`, or `DCBA`.
    h. Allowed Special Characters - Enter allowed special characters, such as `!@#$*`.
    i. Click OK, or continue to the advanced password policy settings.
5. To configure advanced password policy options, click Advanced and configure the following advanced options:
    a. Number of Rules to Comply With - Enter a value or use the up and down arrows to set the number of advanced password policy rules that a user must comply with when

creating a password. The amount of rules that must be complied with cannot be greater than the number of password rules configured.

b. Password Rules - Enter a value or use the up and down arrows to set the number of required types of characters or digits chosen in the corresponding drop-down menu. Use the plus and minus icons to create or delete multiple password rules.

6. Click OK.

9.1.4. Add/Configure Sending Policies

Policies that govern messages sent by users, called sending policies, can be created and modified by an administrator with the Settings Management right. Sending policies enable the administrator to control the types of messages that the users within a domain can send by configuring rules involving file size, encryption, and the maximum lifetime of a message. When sending a simple message, the sending policy configured for the sender's domain is applied. When sending a message within a project, the sending policy configured for the project is applied. Sending policies should be configured after file filtering policies and password policies because administrators can configure sending policies to use a file filtering policy and password policy. Adding a password policy to a sending policy adds constraints to the encryption password entered by the user when encryption is used for uploaded files.

Procedure 9.4. To configure a sending policy:

1. Log in to the Managed File Transfer administration application as an administrator with the Settings Management right.

2. Navigate to the Settings | Policies | Sending Policies page.

3. On the Sending Policies page, choose to Create a New Sending Policy or to Modify, Copy, or Remove an existing sending policy.

4. If the choice was to create a new sending policy or to modify an existing sending policy, on the create a new sending policy page, configure the following sending policy options:

   a. Name, Title, and Description - Enter a name, title, and description for the sending policy. The name will be visible in other parts of the user interface for the administration application, for example, when selecting which sending policy to apply to a domain or a project. Providing detailed information in the name and description fields will make it easier to select the correct sending policy in other parts of the user interface for the administration application. The title will be visible to the users of the domain that the sending policy is applied to. When giving the sending policy a title, select all of the languages used by users in the domain for which the sending policy is configured.

   b. Scope - Choose to make the sending policy available to all domains or available to a single domain by selecting Global or Local to a Domain. If local to a domain is selected, select a domain from the drop-down menu.

   c. Maximum Message Size - Enter a value or use the up and down arrows to set the maximum size allowed for uploaded files of a message. The maximum total message size enables a limit to be put on the total sum of the size of all the files contained in a message. Enter a value or use the up and down arrows to reach the appropriate value.

   d. Enable Anti-Virus - Select this option to enable the anti-virus scan function that analyzes uploaded files. If selected, a Maximum File Scan Size must also be selected.

      Note: Anti-virus scans are system-consuming tasks; scanning files over 1 GB is not recommended.

e. Maximum File Scan for AV Scan - Enter a value or use the up and down arrows to set the maximum size of files that can be scanned. Files that are greater than this value will not be checked for viruses, but will be included in the message.

f. Impose Lifetime - Select this option to impose a default message lifetime. If selected, the message lifetime will always be the default lifetime configured in this policy. Users will not be able to change the lifetime of a message if this option is selected.

g. Default Lifetime - Enter a value or use the up and down arrows to set the default amount of time that will be displayed by default in the file upload form in the user interface. Users will not be able to select a custom lifetime.

h. Maximum Lifetime - Enter a value or use the up and down arrows to set the maximum length of time (in days) that a message lifetime can be configured for in the file upload form in the user interface. This option is not available if a lifetime is imposed.

i. Apply Encryption - Note that the installation of the software 7-Zip is required before being able to use this option. From the drop-down menu, select an encryption policy to apply to the sending policy:

   - Encryption Disabled - The encryption option on the file upload form in the user interface is not available for selection.
   - Encryption Mandatory - The encryption option on the new message form in the user interface is selected and the user cannot disable it.
   - Encryption Optional and Not Suggested - The encryption option on the new message form in the user interface is available, but not selected as the default option.
   - Encryption Optional and Suggested - The encryption option on the new message form in the user interface is available and automatically selected as the default option.

Note

if encryption is enabled, then the path to the `7za` application file must be set in the *`file.encryption.zipExecBinDir`* property (Server Management | Setup | Advanced Settings | Base tab).

---

j. Password Policy - From the drop-down menu, select a password policy to apply to the sending policy. A password policy is only available for selection if encryption is enabled in the sending policy. The drop-down menu is populated by all of the password policies that have been configured to be available for use by the same domain that the sending policy is available to. Select None to configure the sending policy to not require passwords for file encryption.

k. Maximum File Size for Encryption - Use the up and down arrows to adjust the maximum size in MB that a file can be in order to be encrypted and accepted for upload.

l. Allow Encrypted Messages to be Forwarded - Select this option to allow messages containing encrypted files to be forwarded.

m. File Filtering Policy - From the drop-down menu, select a file filtering policy to apply to the sending policy. The drop-down menu is populated by all of the file filtering policies that have been configured to be available for use by the same domain that the sending policy is available to. Select None to configure the sending policy to not use a file filtering policy.

n. Apply Signature - From the drop-down menu, select one of the following options:

- Signature Mandatory - The signature option on the new message form in the user interface is selected and the user cannot disable it. From the drop-down menu, select a configured PDF signature policy to apply to the exchange policy. Selecting this option does not mean that the user must include as least one PDF document among the files of the message being sent; a valid message may contain no PDF document.
- PDF Signature Optional - The signature option on the new message form in the user interface is available, but not mandatory. From the drop-down menu, select a configured PDF signature policy to apply to the exchange policy.
- PDF Signature Disabled - The signature option on the new message form in the user interface is not available for selection.

o. Limit Availability After Download - Select this option to limit the time that a file is available for download by a guest user after the file was downloaded for the first time.

p. Apply Pre-Archiving - From the drop-down menu, select one of the following options:

- Pre-Archiving Disabled - Users will not be able to select the pre-archive option for messages and messages are not pre-archived.
- Pre-Archiving Mandatory - Users will not be able to select the pre-archive option for messages and messages are pre-archived. Then select a Pre-Archiving Policy.
- Pre-Archiving Optional and Not Suggested - Users will be able to select the pre-archive option for messages but the option is not suggested. Then select a Pre-Archiving Policy.
- Pre-Archiving Optional and Suggested - Users will be able to select the pre-archive option for messages and the option is suggested. Then select a Pre-Archiving Policy.

5. To save the configuration, click OK.

9.1.5. Configure Pre-Archiving

MFT includes a pre-archiving functionality for messages and message attachments. A user sending an MFT message can select an option to pre-archive the message upon expiration or deletion. When messages selected to be pre-archived expire or are deleted by a user, the messages remain on the file system and are moved by an asynchronous pre-archiving job to a pre-archiving directory with an XML metadata file that includes message information, such as the subject, content, sent date, download history, view history, recipients, etc. After being pre-archived by MFT, the pre-archived messages can then be exploited by a third-party archiving application.

When messages with encrypted attachments are selected for pre-archiving, the decryption data, in the form of passwords chosen by message senders, are encrypted by a public key and can only be decrypted by the customer in possession of the corresponding private key. The encrypted passwords and encrypted attachments are transferred to the pre-archiving directory in binary files along with the XML metadata file for pre-archived messages. MFT is not capable of decrypting the encrypted data.

An audit log is created each time the pre-archiving job transfers messages to the pre-archiving directory.

Procedure 9.5. To configure a pre-archiving policy:

1. Log in to the MFT administration application as an administrator with the global Settings Management right.

2. Navigate to the Settings | Policies | Pre-Archiving Policies page.

3. On the Pre-Archiving Policies page, choose to Create a New Pre-Archiving Policy or to Modify, Copy, or Remove an existing pre-archiving policy.

4. If the choice was to create a new pre-archiving policy or to modify an existing pre-archiving policy, on the pre-archiving policy configuration page, configure the following pre-archiving policy settings:

    a. Name and Description - Enter a name and description for the pre-archiving policy. The name will be visible in other parts of the user interface for the administration application, for example, when selecting which pre-archiving policy to apply to a sending policy. Providing detailed information in the name and description fields will make it easier to select the correct pre-archiving policy in other parts of the user interface for the administration application.

    b. Scope - Choose the scope of the pre-archiving policy by selecting "Global" or "Local to a Domain." If local to a domain is selected, select a domain from the drop-down menu. If the scope is configured to be local to a domain, the pre-archiving policy will only be available for use within the selected domain. If a pre-archiving policy scope is configured to be global to all domains, the pre-archiving policy will be available for use within all domains.

    c. Pre-Archiving Sub-directory Name - Enter a name for the sub-directory to be used for storing pre-archived messages. The name entered cannot be used by any other pre-archiving policy. The sub-directory will be created on the server hosting the Network File System component of MFT in the `/opt/opentrust/mft/var/mnt/files/prearchiving` file path. Within the sub-directory, additional sub-directories named after message identifiers will be created for each pre-archived message and any attachments.

    d. Pre-Archive Encrypted Messages - Choose to enable or disable pre-archiving of encrypted messages. If pre-archiving of encrypted messages is enabled, configure the following additional options:

        i. Passphrase Encryption Certificate - Select a certificate from the drop-down menu. All certificates that have been registered in the Server Management | Certificates and Keys | Trusted Certificates menu will be available for selection. The selected certificate will be used to encrypt the user-selected passwords of encrypted messages when the encrypted messages are moved to the pre-archiving directory.

        ii. Executable File Format - Choose to package the encrypted messages in Windows or Linux binary files. In both cases, decryption requires the password selected by the message sender when an encrypted message was sent.

Note

If the option is disabled after messages have been sent, the previously sent messages will be encrypted; in other words, the enabled/disabled status at the time of message sending is applied.

---

5. To save the configuration, click OK. The pre-archiving policy is now available for selection in sending policies that correspond to the configured scope of the pre-archiving policy.

9.2. Configure Exchange Settings

Exchange Policy settings enable an administrator to create specific rules and guidelines for how individual users will be able to interact within the Managed File Transfer application. Administrators can configure exchange rules to create exchange policies that are used to specify how the user it will be applied to can interact with other users. Exchange rules should be created before exchange policies. After being configured, an exchange policy can be applied to the appropriate user by an administrator with the User Management right by editing the user, as described in Chapter 5, Manage Users.

The user will not have the "Send" tab on the end user application unless the exchange policy attached to the user is configured to allow the user to send messages and be involved in projects. Under the "Send" tab, if the user policy is only configured to allow for simple messages to be sent, only that option will be visible on the end user application. Or, if the user policy is only configured to allow for projects, the simple messages option will not be visible, but the project option will. This makes it clear to the user what is allowed according to their specific exchange policy.

The scope of an exchange rule or policy can be configured as either global to all domains or local to a domain. Exchange rules and policies that are global to all domains will be visible and available for use when configuring users within any domain. Local exchange rules and policies will only be visible and available for use when configuring users within the domain selected during the configuration of the exchange rule or policy. Most exchange rules and policies can be configured by an administrator with the Global Settings Management or the Local Settings Management right to the selected domain. However, an administrator creating an exchange rule for exchanges with registered users must have the Global Settings Management right.

In this section, administrators can:

- Section 9.2.1, “Create an Exchange Rule”
- Section 9.2.2, “Create an Exchange Policy”3

9.2.1. Create an Exchange Rule

There are two types of exchange rules that can be configured to be applied to an exchange policy. Administrators can create rules to control a users exchanges with either other registered users or with guest users.

9.2.1.1. Define Exchanges with Registered Users

Procedure 9.6. To configure a rule for exchanges with registered users:

1. Log in to the Managed File Transfer administration application as an administrator with the Global Settings Management right.
2. Navigate to the Settings | Policies | Rules for Exchanges with Registered Users page.
3. On the Rules for Exchanges with Registered Users page, choose to Create a New Exchange Rule or to Modify, Copy, or Remove an existing exchange rule.
4. If the choice was to create a new exchange rule or to modify an existing exchange rule, on the create a new exchange rule page, configure the following exchange rule options:
    a. Name, Title, and Description - Enter a name, title, and description for the exchange rule. The name will be visible in other parts of the user interface for the administration application, for example, when selecting which exchange rule to apply to a exchange policy. Providing detailed information in the name and description fields will make it easier to select the correct exchange policy in other parts of the user interface for

the administration application. When giving the exchange rule a title, select all of the languages used by users in the domain for which the exchange rule is configured.

b. Scope - Choose to make the exchange rule available to all domains or available to a single domain by selecting Global or Local to a Domain. If local to a domain is selected, select a domain from the drop-down menu.

c. Allowed MFT Domains - From the drop-down menu, select the Managed File Transfer domains within which users can send messages to:

   - All Domains - Allows users to send messages to all users in all domains configured in the Managed File Transfer application.
   - User Domain - .
   - No Access - Restricts users from sending messages to any users within any domain configured in the Managed File Transfer application.
   - Custom - From the drop-down menu, select a Managed File Transfer domain. To select multiple domains in the list, use the Ctrl key. All configured Managed File Transfer domains will be available for selection in the drop-down menu. Users will be able to send messages only to the selected domains.

d. Email Domains - From the drop-down menu, select the email domains users can send messages to. Customizing available email domains enables the administrator to further refine to whom the user can send messages to within the already selected Managed File Transfer domains:

   - All Email Domains - Allows users to send messages to all email addresses within the Managed File Transfer domains selected in the Allowed MFT Domains option.
   - User Domain - Allows users to send messages only to users within their own domain.
   - Custom - If custom is selected, enter the email domains that users will be allowed to send messages to. The special character * is allowed as long as it is not the last entry in the email domain name. A domain name must begin with an @ symbol. To enter multiple email domains, place a carriage return between each entry. For example:

```
@acme.com
@*.acme.com
```

e. Auto-complete Scope - Auto-completion is used to generate a list of email addresses that match the address a user is typing as the recipients to a message are being entered or when selecting members to include in a project. The default setting is to include only the same email addresses that the user is allowed to send a message to or add to a project in the auto-completion list. However, in certain circumstances, when the goal is to restrict the visibility of the email addresses displayed in the suggestion list, an administrator may choose to configure the list so that a user could be allowed to send a message to certain users that will not be displayed in the auto-completion suggestion list. To configure a policy for the auto-completion list other than the default setting, from the drop-down menu select one of the following options:

   - No Access - Auto-complete will be turned off and the user sending the files must enter the full email address of the recipients.
   - User Domain - Only email addresses that correspond to users within the user's own domain will be available in the auto-complete list.
   - Custom - The administrator must select from the list which email domains to include in the auto-complete list.

5. Click OK.

9.2.1.2. Define Exchanges with Guest Users

Procedure 9.7. To configure a rule for exchanges with guest users:

1. Log in to the Managed File Transfer administration application as an administrator with the global or local Settings Management right.

2. Navigate to the Settings | Policies | Rules for Exchanges with Guest Users page.

3. On the Rules for Exchanges with Guest Users page, choose to Create a New Exchange Rule or to Modify, Copy, or Remove an existing exchange policy.

4. If the choice was to create a new exchange rule or to modify an existing exchange rule, on the create a new exchange rule page, configure the following exchange policy options:

    a. Name, Title, and Description - Enter a name, title, and description for the exchange rule. The name will be visible in other parts of the user interface for the administration application, for example, when selecting which exchange rule to apply to an exchange policy. Providing detailed information in the name and description fields will make it easier to select the correct exchange policy in other parts of the user interface for the administration application. When giving the exchange rule a title, select all of the languages used by users in the domain for which the exchange rule is configured.

    b. Scope - Choose to make the exchange policy available to all domains or available to a single domain by selecting Global or Local to a Domain. If local to a domain is selected, select a domain from the drop-down menu.

    c. Email Domains - From the drop-down menu, select the email domains users will be allowed to send messages to outside of the Managed File Transfer application:

        - All Email Domains - Allows messages to be sent to all email domains.

        - User Domain - Allows users to only send messages to email addresses with the same domain as the user's email address.

        - No Access - Restrict messages from being sent to any email domain.

        - Custom - If custom is selected, enter the email domains that users will be restricted from sending messages to. The special character * is allowed as long as it is not the last entry in the email domain name. A domain must begin with a @ symbol. To enter multiple email domains, place a carriage return between each entry. For example:

        ```
        @acme.com
        @*.acme.com
        ```

5. Click OK.

9.2.2. Create an Exchange Policy

Exchange policies can be configured by administrators with the global or local Settings Management right. Exchange policies are applied to individual users and are designed to control the rights that each user has to exchange with other registered users and guest users. Exchange polices can be customized by using different exchange rules for each policy, as described in Section 9.2.1, “Create an Exchange Rule”

Procedure 9.8. To configure an exchange policy:

1. Log in to the Managed File Transfer administration application as an administrator with the global or local Settings Management right.

2. Navigate to the Settings | Policies | Exchange Policies page.

3. On the Exchange Policies page, choose to Create a New Exchange Policy or to Modify, Copy, or Remove an existing exchange policy.

4. If the choice was to create a new exchange policy or to modify an existing exchange policy, on the create a new exchange policy page, configure the following exchange policy options:

    a. Name and Description - Enter a name and description for the exchange policy. The name will be visible in other parts of the user interface for the administration application, for example, when selecting which exchange policy to apply to a user. Providing detailed information in the name and description fields will make it easier to select the correct exchange policy in other parts of the user interface for the administration application.

    b. Scope - Choose to make the exchange policy available to all domains or available to a single domain by selecting Global or Local to a Domain. If local to a domain is selected, select a domain from the drop-down menu.

    c. Rule for Messages to Registered Users - From the drop-down menu, select the rule which will control the registered users to whom the user is allowed to send simple messages. All configured rules for exchanges with registered users that have been configured for the domain applicable to the exchange policy will be available.

    d. Rule for Messages to Guest Users - From the drop-down menu, select the rule which will control the guest users to whom the user is allowed to send simple messages to. All configured rules for exchanges with guest users that have been configured for the domain applicable to the exchange policy will be available.

    e. Maximum Number of Guest Recipients - From the drop-down menu, choose whether or not to set a limit for the maximum number of guest recipients. If the choice was to set a limit, enter a value in the text box, or use the up and down arrows to configure the limit.

    f. Project Creation Authorization - Select this option to grant the user authorization to create new projects. The user will only have the ability in the end-user application to create projects if this option is configured.

    g. Rule for Project Members Management - From the drop-down menu, select the rule which will control the registered users that the user is allowed to add to a managed project. All configured rules for exchanges with registered users that have been configured for the domain applicable to the exchange policy will be available.

    h. Rule for Upload Tokens Creation - From the drop-down menu, select the rule which will control the guest users to whom the user can send upload tokens to. All configured rules for exchanges with guest users that have been configured for the domain applicable to the exchange policy will be available. The user will only have the ability in the end-user application to upload tokens if this option is configured.

5. Click OK.

9.3. Create/Upload Themes

A theme can be created and set to control the presentation of the end under application by customizing features such as the logo or the banner.

In this section, administrators can:

- Section 9.3.1, “Create a Theme”
- Section 9.3.2, “Upload a Theme”

9.3.1. Create a Theme

The creation of an MFT theme requires some knowledge of CSS (Cascading Style Sheets) and its application to WEB page styling. Use of specialized software to edit CSS files is not mandatory but strongly recommended. Also, it may be necessary to use a browsers built in facilities or extensions to analyze the MFT web pages structure and styles (for example, the Firebug extension for Firefox).

9.3.1.1. Theme structure

An MFT theme is structured as a directory that holds all of the resources (CSS files, images...) that are necessary to the theme. All resources must be stored at the directory's root (sub-directories are forbidden). The only mandatory theme element is a `theme.css` file. This file can reference other CSS files or graphical resources.

A `theme_login.css` file can also be provided to customize the end user login page.

Finally, the following HTML files can also be provided, to customize the footer pages of the application: `footer.html`, `footer_token.html`, `footer_login.html`.

Typically, the following files may be part of an MFT theme:

- theme.css (general customization of the end user interface)
- theme_login.css (customization of the end user interface login page)
- logo.png (logo image inserted on the main end user interface page)
- footer.html (footer HTML elements inserted in the main end user interface page)
- footer_login.html (footer HTML elements inserted in the end user interface login page)
- footer_token.html (footer HTML elements in the end user interface token pages - upload and download)
- logo.gif (logo image inserted on the main end user interface page on Internet Explorer 6 only)
- header.jpg (used as a background gradient behind the product logo on the main end user interface page)
- header-background.jpg (used on the right hand side and left hand side of the logo on the main end user interface page)

The `theme.css` and `theme_login.css` are included in the WEB page after the built in theme. Thus, it is only necessary to override the built in theme, and not to reimplement the whole page styling.

Below is a snippet of HTML code that demonstrates how the various CSS files are loaded, when the "OpenTrust" theme is applied:

```
<html>
```

```
  <head>
    <meta http-equiv="content-type" content="text/html; charset=UTF-8"/>
    <meta http-equiv="X-UA-Compatible" content="IE=9"/>
    <meta name="gwt:property" content="locale=fr"/>

    <title>OpenTrust MFT</title>

    <link rel="SHORTCUT ICON" href="/mft-webapp-user/favicon.ico"/>
    <link type="text/css" rel="stylesheet" href="/mft-webapp-user/loading.css"/>
    <link type="text/css" rel="stylesheet" href="/mft-webapp-user/style.css"/>

    <link type="text/css" rel="stylesheet" href="themes/OpenTrust/theme.css"/>
```

Note that the `theme.css` file is loaded last from the directory corresponding to the "OpenTrust" theme.

9.3.1.2. Languages

Depending on the language, some text localization may require that the page layout be adapted. For example, some labels may be much longer in French than in English, which will require that a minimum size for a dialog box be set to a bigger value.

To set CSS entries specific to a language, one can use the `.lang` selector, where `lang` is the corresponding language code. For example:

```
.fr .header {
min-width: 1020px;
}
.fr .wrap {
    min-width: 990px;
}
.fr .file {
    padding-right: 560px;
}
.fr .file-date {
    width: 205px;
}
.fr .file-info {
    right: 225px;
    width: 315px; }
```

9.3.1.3. Customizable elements

In theory, all visual elements can be customized, since we are only overriding the built in theme. However for practical reasons, it is more reasonable to only override some of the following elements in the WEB page.

9.3.1.3.1. Header

The page's header is the most obvious candidate for theme ability. Most of the time, the following elements will be changed:

- the header background image or color
- the header logo (to be replaced with your company's logo, for example)
- the header's height (to be increased or decreased, depending on the logo size for example)

To do all this, a `logo.png` should be uploaded in the theme and the following CSS entries should be put in the `theme.css` file:

```
.header {
    background: #fff;
    height: 130px;
}
.header-wrap {
    background: #fff ;
    height: 130px ;
}
.logo {
    background-image: url("logo.png") ;
    width: 368px;
    height: 84px;
}
```

In the example above:

- the `header` class override sets a white background, and a height reduced to 130px that must be equal to the height of header-wrap.
- the `logo` class override sets the image used as the background logo. Note the reference to the `logo.png` file.

Please notice the access path to the `logo.png` file: giving a complete path is not necessary and not recommended, since resources are referenced in paths relative to the CSS file itself.

9.3.1.3.2. Main tabs

The main tabs are those dedicated to the Messages, Search and Send functions. One may want to change the text's color when the tab is selected. One may also want to change the color of an activated filter element (such as All, New, etc.) in the filter bar on the Messages tab.

To achieve this, the following entries should be put in the `theme.css` file:

```
.tabs a {
    color: #CC8888;
}

.tabs on {
    color: #CC0000;
}

.filter a.on {
    color: #CC0000;

}
```

In the example above:

- The `tabs` class is mapped to the actual tabs container and the default color was changed to #CC8888.
- The on class is applied inside the `tabs` container to the active tab and the selected color was changed to #CC0000.
- The `filter` class is mapped to the container of all filter elements (which are anchors) and the color of selected elements inside this container was changed to #CC0000.

9.3.1.4. Tips

The `style.css` built in style sheet can be downloaded at the following URL:

```
https://mymftserver/zephyr/style.css
```

After having downloaded and installed Firefox, install the `Firebug` extension. This extension enables you to study the HTML and CSS styles applied to a whole web page, and make live changes to both the HTML and CSS.

`Firebug` is a very powerful tool that will be helpful when trying to quickly put a new MFT Theme together and when performing any of the following related actions:

- Identifying the element that must be customized
- Inspecting the element with Firebug
- Making the necessary modifications to the element's style and reviewing the results live
- Copying the modifications back to the `theme.css` file.

9.3.1.5. Annex

An example of a theme.css file:

```
.header {
    background: URL(header-background.jpg);
    height: 140px;
}

.header-wrap {
 background: URL(header.jpg)no-repeat scroll center top transparent;
    height: 140px;
}

/* Product logo */

.logo {
    background-image: url(logo.png);
    width: 368px;
    height: 84px;
}
/*** Locale: fr and ru ***/

.fr .header, .ru .header {
    min-width: 1020px;
}
.fr .wrap, .ru .wrap {
    min-width: 990px;
}

.fr .file, .ru .file {
    padding-right: 560px;
}
.fr .file-date, .ru .file-date {
    width: 205px;
}
.fr .file-info, .ru .file-info {
    right: 225px;
    width: 315px;
}
.ru .popup-message {
    width: 470px;
}
```

An example of theme_login.css file:

```
.login {
        background: url(logo-header-background.png) repeat-x scroll center top transparent;
}

.login .wrap {
        background: url(login-header.png) no-repeat scroll center top transparent;
        margin: 0 auto;
        min-width: 0;
        padding: 231px 10px 40px;
        width: 900px;
}
```

An example of a footer.html file:

The content is the same for the `footer.html`, `footer_token.html` and `footer_login.html`.

```
<div class="footer">
  <div class="wrap">
    <a class="footer-logo" href="http://www.opentrust.com/"
       target="_blank">OpenTrust</a>
  </div>
  </div>
```

9.3.2. Upload a Theme

Themes enable an administrator with the global or local Settings Management right to control the presentation of the end application by customizing features such as the logo or the banner.

Procedure 9.9. To upload a Theme:

1. Log in to the Managed File Transfer administration application as an administrator with the Settings Management right.
2. Navigate to the Settings | Domains | Themes page.

3. On the Themes page, choose to Create a New Theme or to Modify, Copy, or Remove an existing theme.
4. If the choice was to create a new theme or to modify an existing theme, on the create a new theme page, configure the following theme settings:
    a. Name and Description - Enter a name and description for the theme. The name will be visible in other parts of the user interface for the administration application, for example, when selecting which theme to use for a particular domain. Providing detailed information in the name and description fields will make it easier to select the correct theme in other parts of the user interface for the administration application.
    b. Scope - Choose to make the theme available to all domains or available to a single domain by selecting Global or Local to a Domain. If local to a domain is selected, select a domain from the drop-down menu.
    c. Click OK.
    d. In the Edit Theme box, select to Download all Files (as ZIP) or to Add Files.
    e. If the choice was to add files, in the pop-up box, select Browse.
    f. From the File Upload box, select a theme.css file to correspond to the configured theme.

        Note: The theme will not work correctly without uploading a theme.css file. All graphical resources referenced by "theme.css" must be located under the same directory as the "theme.css"; subdirectories are not supported.
    g. Click Upload.
    h. In the Edit Theme box, click to Download All Files.
    i. Click OK.

9.4. Configure Repositories

Administrators can configure the following to enable the use of repositories:

- Section 9.4.1, “Configure User Providers”
- Section 9.4.2, “Configure Datasources”
- Section 4.1, “Configure an LDAP Directory Connection”
- Section 9.4.3, “Configure Contact Sources”

9.4.1. Configure User Providers

User providers can be used to create, update, and delete user accounts.

User providers configured to use LDAP datasources determine how the data retrieved from an LDAP directory user source repository can be used to enable the creation of user accounts, can be used to authenticate users, and can be used to create contact sources.

File import user providers have the following limitations: they cannot be used to create user accounts, cannot be used to authenticate users, and cannot be used as contact sources. File import user providers simply determine the how the data retrieved from an uploaded file user source repository is mapped into the user accounts created by uploading the file.

Procedure 9.10. To configure a user provider:

1. Log in to the MFT administration application as an administrator with the Settings Management right.
2. Navigate to the Settings | Repositories | User Provider page.
3. On the User Provider page, choose to Create a New User Provider or to Modify, Copy, or Remove an existing user provider.
4. If the choice was to create a new user provider or to modify an existing user provider, on the user provider configuration page, configure the following user provider settings:
    a. Name and Description - Enter a name and description for the user provider. The name will be visible in other parts of the user interface for the administration application, for example, when selecting which contact source to use for a particular domain. Providing detailed information in the name and description fields will make it easier to select the correct contact source in other parts of the user interface for the administration application.
    b. Scope - Choose the scope of the user provider by selecting "Global" or "Local to a Domain." If local to a domain is selected, select a domain from the drop-down menu. If a user provider scope is configured to be local to a domain, only datasources configured to be local to the selected to domain or global to all domains will be available for selection in the Datasource drop-down menu. If a user provider scope is configured to be global to all domains, only datasources configured to be global to all domains will be available for selection in the Datasource drop-down menu.
    c. Active - Choose whether to make the user accounts created by this user provider active. If a user provider is deactivated after the user provider has been used to create user accounts, the users created with the user provider will no longer be able to login, but will still be active users. No new users will be created by a non-active user provider.
    d. Datasource - Select a configured datasource from the drop-down menu. All datasources that have been configured as described in Section 9.4.2, “Configure Datasources” and correspond to the configured scope for the user provider will be available for selection, as will the pre-configured File Import datasource.
    e. Additional LDAP Datasource Options:
        - Use as Contact Source - use attribute values retrieved from the LDAP directory to auto-complete message recipient entries
        - Use as Authentication Scheme - use attribute values retrieved from the LDAP directory and the selected password handling option to authenticate users
        - User Data Refresh Interval - the frequency with which user data is retrieved from the LDAP directory
    f. Default User Domain - If a domain is not determined by the user mapping, the provsionned user will have the default user domain as a domain.
    g. User Mappings - In the available fields for the attributes from the selected datasource, drag and drop the datasource and/or free-form text fields from the palette to the corresponding user provider fields. The palette is displayed (it slides from left to right) when the mouse hovers the left side of the screen. Refer to the tooltips in the UI for additional information on individual fields.

        When configuring a file import datasource, certain datasource field attributes such as those containing "other" can be used to map values from the temporary uploaded file that do not correspond to an expected use, but the datasource field attributes "UID"

and "email" must always be mapped to correctly correspond to the UID and email address values provided in the temporary uploaded file.

5. To save the configuration, click OK. When the configuration is saved for LDAP user providers, user data retrieved from the LDAP directory is immediately available for use by MFT. When the configuration is saved for file import user providers, user data should then be uploaded as described in Section 5.3, “Add and Synchronize Registered Users By File Upload”.

6. If the configuration was saved for LDAP user providers with the "Use as Authentication Scheme" option selected, administrators can now configure an authentication policy to use this user provider and set the default authentication policy on the related MFT domains.

9.4.2. Configure Datasources

User source repositories, including LDAP directories or uploaded files, can provide user information to MFT, such as user names, UIDs, email addresses, passwords, and other user attributes. Datasource configurations determine the user data to retrieve from user source repositories for use by MFT and, to a limited extent, determine how the retrieved data will be used by MFT, such as to a identify a user or to search for a user.

Administrators can configure LDAP datasources that use an LDAP directory integrated with MFT as the user source repository or use the pre-configured and unmodifiable file import datasource that uses a temporary uploaded file as the user source repository. For additional information on how to configure a connection to an LDAP directory that will be used as a user source repository, refer to Section 4.1, “Configure an LDAP Directory Connection”. For additional information on how to upload a temporary file that will be used as a user source repository and synchronization method, refer to Section 5.3, “Add and Synchronize Registered Users By File Upload”. In the LDAP datasource configurations, as described in this section, administrators can configure the attributes retrieved from the user source repository and used by MFT. The pre-configured and unmodifiable file import datasource can retrieve and use the attributes included in the "Datasource Fields" section of the palette used to configure a user provider on the Settings | Repositories | User Providers page of the UI, which is described in Section 9.4.1, “Configure User Providers”.

Procedure 9.11. To configure an LDAP datasource:

1. Log in to the MFT application as an administrator with the Global System Setup Settings Management right.

2. Navigate to the Settings | Repositories | Datasources page.

3. On the Datasources page, choose to Create a New LDAP Datasource, to Modify, Copy, or Remove an existing LDAP datasource.

Note

An LDAP datasource cannot be removed if it is in use.

---

4. If the choice is to create a new LDAP datasource or modify or copy an existing LDAP datasource, on the LDAP Datasource page, configure the following LDAP datasource options:

   a. Name and Description - Enter a name and description for the LDAP datasource. The name and description will be visible in other parts of the user interface, for example, when selecting which LDAP datasource to use for a particular card management profilecertificate management profile. Providing detailed information in the name and

description fields will make it easier to select the correct LDAP datasource in other parts of the user interface.

b. Scope - Choose the scope of the datasource by selecting "Global" or" Local to a Domain." If local to a domain is selected, select a domain from the drop-down menu. If a datasource scope is configured to be local to a domain, only LDAP directory connections configured to be local to the selected to domain or global to all domains will be available for selection in the Directory drop-down menu. If a datasource scope is configured to be global to all domains, only LDAP directory connections configured to be global to all domains will be available for selection in the Directory drop-down menu.

c. Connection Settings - Select the search criteria to use when the server application connects to the LDAP datasource:

- Directory - Select a configured LDAP directory connection from the drop-down menu. All LDAP directory connections that have been configured as described in Section 4.1, "Configure an LDAP Directory Connection" and correspond to the configured scope for the datasource will be available for selection.
- Search Constraints - This is a generic attribute and value user search filter, without surrounding parenthesis. Administrators typically enter: `&(objectclass=person)(uid=*)`
- Use DN Components - Select this option to include DN components in the list of values returned in the search result sample.
- Test Search - Enter an attribute and value for performing a directory test search, without surrounding parenthesis. Administrators typically enter: `uid=`*`jdoe`*, where *`jdoe`* is the `uid` value of an entry in the LDAP directory.

5. Click Search.
6. The search results are a list of user entry attributes from a sample datasource entry matching the search criteria entered in the Connection Settings options. If the search criteria option to Use DN Components was selected, the DN component attributes are displayed in the DN Components section of the table. To select the fields available during searches and communication with MFT and to determine which LDAP attributes will be available to MFT, in the DN Components and LDAP Attributes sections of the table, select LDAP attributes and their corresponding options and values. Use the More Details/Less Details toggle to display more or less LDAP attributes. For descriptions of the columns, mouse over each column name.
7. Click Save.

Note

Once a datasource has been saved, an administrator cannot deselect the associated identifiers. To choose different identifiers, a new datasource must be created. If messages have not yet been sent using the datasource, administrators can delete the datasource.

9.4.3. Configure Contact Sources

Contact sources can be created by administrators with the Settings Management right. Contact sources work as an addition to the registered-user database for the auto-complete function in the end-user application. Configuring contact sources enables an administrator to create a more complete contact list for the auto-complete function. Simple SQL database or LDAP contact source plug-ins must be configured, as described in Section 4.2, "Configure Authentication or

Contact Source Plug-ins", before contact sources can be fully configured. After a contact source has been configured, the contact source can be selected for use by a domain, as described in Chapter 3, Configure Domains.

Procedure 9.12. To configure a contact source:

1. Log in to the Managed File Transfer administration application as an administrator with the Settings Management right.
2. Navigate to the Settings | Repositories | Contact Sources page.
3. On the Contact Sources page, choose to Create a New Contact Source or to Modify, Copy, or Remove an existing contact source.
4. If the choice was to create a new contact source or to modify an existing contact source, on the contact source configuration page, configure the following contact source settings:
    a. Name and Description - Enter a name and description for the contact source. The name will be visible in other parts of the user interface for the administration application, for example, when selecting which contact source to use for a particular domain. Providing detailed information in the name and description fields will make it easier to select the correct contact source in other parts of the user interface for the administration application.
    b. Scope - Choose the scope of the contact course by selecting Global or Local to a Domain. If local to a domain is selected, select a domain from the drop-down menu.
    c. Contact Source Plug-ins - From the drop-down menu, select a contact source plug-in. As many contact sources as necessary can be selected. If contact source plug-ins have not yet been configured, this step cannot be completed.
5. Click OK.

9.5. Configure Additional Settings

Administrators with the Settings Management right have the ability to configure additional settings to further customize the needs of the users within a domain. After an additional setting is configured, an administrator with the Domain Management right can edit a domain to use the setting, as described in Chapter 3, Configure Domains. Like other policies, the scope of any additional setting can be configured as either global or local to a domain. Global settings will be visible and available for use to all domains and can only be configured by an administrator with the Global Settings Management right. Settings with a scope local to a domain will only be visible and available for use to the domain selected during configuration of the setting and can only be configured by an administrator with the Local Settings Management right for the selected domain or with the Global Settings Management right.

In this section, administrators can:

- Section 9.5.1, "Add/Configure Information Messages"
- Section 9.5.2, "Add/Configure Email Templates"
- Section 9.5.3, "Manage Scheduled Jobs"

9.5.1. Add/Configure Information Messages

Information messages enable administrators with the Settings Management right to configure a message that will be displayed to users in a domain upon login or when password reset is

required. An administrator can configure the same message to be displayed at each login over a long period of time or create new messages as often as needed.

Procedure 9.13. To configure an Information Message:

1. Log in to the Managed File Transfer administration application as an administrator with the Settings Management right.
2. Navigate to the Settings | Domains | Information Messages page.
3. On the Information Messages page, choose to Create a New Information Message or to Modify, Copy, or Remove an existing information message.
4. If the choice was to create a new information message or to modify an existing message, on the create a new information message page, configure the following message:
    a. Name and Description - Enter a name and description for the information message. The name will be visible in other parts of the user interface for the administration application, for example, when selecting which message of the day to use for a particular domain. Providing detailed information in the name and description fields will make it easier to select the correct message of the day in other parts of the user interface for the administration application.
    b. Scope - Choose to make the information message available to all domains or available to a single domain by selecting Global or Local to a Domain. If local to a domain is selected, select a domain from the drop-down menu.
    c. Start Date and End Date - From the corresponding drop-down menus, select the date for when the message should begin to be displayed and the date that the message should no longer be displayed.
    d. Language - From the drop down menu, select the language the message will be displayed in.
    e. Message - Type the full information message in the text box. Everything entered within the text box will be displayed in the information message. The language the message is typed in must be the language selected in the language parameter.
5. Click OK.

9.5.2. Add/Configure Email Templates

Email templates enable an administrator with the global or local Settings Management right to create automatic emails that will be sent to select users for events that take place in the Managed File Transfer application. The email template will create an identically formated email that will be sent to the selected recipients each time the chosen event occurs within the selected domain. Administrators can choose to create a unique email template or choose an existing, pre-formated template to modify and use.

When sending an email that uses an email template to a user, Managed File Transfer will try to find the localized email template that matches each individual email recipient's language. If the email recipient's language is unknown, Managed File Transfer will apply the following fall-back rules to find an alternate localized email template for the recipient:

- For registered user recipients
    1. The language preference of the user.
    2. The default language configured for the user's domain.

- For guest user recipients

  1. The language configured in the address book entry of the creator of the user's token.

  2. The default language preference of the token creator.

  3. The default language configured in the token creator's domain.

If no localized email template can be found, the following global fall-back rules will apply:

- Managed File Transfer will attempt to find a localized email template for the language configured in the Advanced Settings setting property "i18n.defaults.lang."

- Managed File Transfer will use the first language available in the email template.

Procedure 9.14. To configure an email template:

1. Log in to the Managed File Transfer administration application as an administrator with the Settings Management right.

2. Navigate to the Settings | Domains | Email Templates page.

3. On the Email Templates page, choose to Create a New Email Template or to Modify, Copy, or Remove an existing email template..

4. If the choice was to create a new email template, select a pre-formated email template, or on the create a new email template page, configure the following email template settings:

   a. Name and Description - Enter a name and description for the email template. The name will be visible in other parts of the user interface for the administration application, for example, when selecting which email template to use for a particular domain. Providing detailed information in the name and description fields will make it easier to select the correct email template in other parts of the user interface for the administration application.

   b. Scope - Choose to make the email template available to all domains or available to a single domain by selecting Global or Local to a Domain. If local to a domain is selected, select a domain from the drop-down menu.

   c. Event - From the drop-down menu, select one of the following events to trigger the automatic notification email to be sent every time the selected event occurs:

      i. Message Lifecycle :

         - Message Sent to a Registered User - Select this option to send a notification email every time a message is sent by a registered user to another registered user.

         - Message Sent in a Project - Select this option to send a notification email every time a message is sent within a project.

         - Message Sent to a Guest User - Select this option to send a notification email every time a message is sent by a registered user to a guest user.

         - Message Sent Using an Upload Token - Select this option to send a notification email every time a message is sent by an guest user to a registered user using an upload token.

         - Message Viewed by a Registered User - Select this option to send a notification email every time a message sent to a registered user is viewed by the receiver.

- Message Viewed by a Registered User in a Project - Select this option to send a notification email every time a message sent within a project is viewed by one of the registered users within the project.
- Message Viewed by a Guest User - Select this option to send a notification email every time a message sent to a guest viewer is viewed by the receiver.
- Download by a Registered User - Select this option to send a notification email every time a registered user downloads a file sent directly by another registered user.
- Download by a Registered User in a Project - Select this option to send a notification email every time a registered user downloads a file sent within a project.
- Download by a Guest User - Select this option to send a notification email every time a guest user downloads a file sent directly by a registered user.
- Message Deletion for a Registered User - Select this option to send a notification email every time a message sent to a registered user is deleted by the receiver.
- Message Deletion in Project for Registered User - Select this option to send a notification email every time a message sent within a project is deleted by a registered user.
- Message Deletion for a Guest User - Select this option to send a notification email every time a message sent to a guest user is deleted by the receiver.

ii. Message Reminder :

- First Message Reminder Sent to a Registered User - Select this option to send the first notification email every time a message sent to a registered user by any other user is about to expire.
- Second Message Reminder Sent to a Registered User - Select this option to send the second notification email every time a message sent to a registered user by any other user is about to expire.
- First Message Reminder in a Project - Select this option to send the first notification email every time a message sent within a project is about to expire.
- Second Message Reminder in a Project - Select this option to send the second notification email every time a message sent within a project is about to expire.
- First Message Reminder to a Guest User - Select this option to send the first notification email every time a message sent to a guest user is about to expire.
- Second Message Reminder to a Guest User - Select this option to send the second notification email every time a message sent to a guest user is about to expire.
- First Message Reminder Sent by a Guest User - Select this option to send the first notification email every time a message sent by a guest user to a registered user is about to expire.
- Second Message Reminder Sent by a Guest User - Select this option to send the second notification email every time a message sent by a guest user is about to expire.

iii. Upload Token Lifecycle :

- Upload Token Creation - Select this option to send a notification email every time an upload token is created.
- Upload Token Deletion - Select this option to send a notification email every time an upload token is deleted.

iv. Project Lifecycle :

- User Added to Project - Select this option to send a notification email every time a user is added as participant to a project (during a project creation or afterward).
- User Removed from Project - Select this option to send a notification email every time a user removed from the project participants.
- Project Deletion - Select this option to send a notification email every time a project is deleted.

v. User Lifecycle :

- User Creation - Select this option to send a notification each time a new user account is created.
- Quota Increase Requested by User - Select this option to send a notification each time a user requests a quota increase on the end user application.
- User Deletion - Select this option to send a notification each time a user account is deleted.
- User Expiration - Select this option to send a notification each time a user account expires.
- Inactive User Deactivation - Select this option to send a notification each time an inactive user is deactivated.
- User Password Reset Request - Select this option to send a notification each time a user request a password reset on the end user application.
- User Password Changed By Administrator - Select this option to send a notification each time a user password is changed by an administrator.

d. From - From the drop-down menu, select an email address to use for the sender of the automatic notification email. The sender options will vary depending on the event selected. To use a customized address that is different from the choices available, select Fixed and enter an email address in the text box.

e. Recipients - From the drop-down menu, select which recipients should receive the email message. Or, in the empty box, type a customized email address for the recipient. If the emails will be sent to more than one recipient, use the add and subtract icons to adjust the number of boxes available to select recipients or enter customized email addresses. The recipient options will vary depending on the event selected.

f. Language - From the drop-down menu, select which language the mail notification should be in.

g. Variables - From the drop-down menu, select a component variable and use the corresponding Add icons to place the component variables within the template.

h. Subject - In the text box, enter the subject of the mail notification or use component variables for the subject.

i. Plain Text Body - In the text box, enter the body of the email as it will appear in plain text, or use the component variable option to make up the body.

j. HTML Body - In the text box, enter the body of the email as it will appear in HTML form, or use the component variable option to make up the body.

5. Click OK.

9.5.3. Manage Scheduled Jobs

The scheduled jobs function of the Managed File Transfer server application allows an administrator with the System Management right to manage jobs. Most scheduled jobs are required to run on a regular basis in order for the Managed File Transfer server application to run appropriately. They should only be unscheduled or rescheduled under the direction of an assigned Equisign technical contact.

Procedure 9.15. To schedule a new job:

1. Log in to the Managed File Transfer administration application as an administrator with the System Management right.

2. Navigate to the Server Management | System | Scheduled Jobs page.

3. On the Scheduled Jobs page, choose to Create a New Job or to Modify, Reschedule, Run, or Remove an existing scheduled job.

4. If the choice was to create a new job or to modify an existing job, on the create a new job page, configure the following job settings:

   a. Job Name and Description - Enter a name and description for the scheduled job. The name and description of the job will be visible in other parts of the user interface for the administration application, such as when managing configured scheduled jobs. Provided detailed information in the job name and description will make it easier to select the correct job when managing scheduled jobs.

   b. Scheduled - Select this option to activate the job to be scheduled.

   c. Implementation Class Name - In the text box, enter the implementation class name. The class referenced by the class name must implement the interface JobTask. The class will be responsible for performing the action associated with this job.

   d. Cron Expression - From the drop-down menu, choose to configure the cron expression in a guided form or raw form. If Guided is selected, enter the time required in each field. The cron expression defines when a scheduled job runs automatically. Refer to the tool tip in the user interface for more specific instructions.

   e. Click OK.

Chapter 10. Reporting and Audit Logs

In this section, administrators can:

- Section 10.1, “Reporting”
- Section 10.2, “Use the Audit Logs User Interface”

10.1. Reporting

The search for reports function enables administrators to search and view two different types of reports.

In this section, administrators can:

- Section 10.1.1, “View User Reports”
- Section 10.1.2, “View Activity Reports ”

10.1.1. View User Reports

The User Reports function enables an administrator to generate user reports on users in the domain that they have the User Audit right over. The search results will allow the administrator to view various information on all the users they have the User Audit right over in a simple form. To view all users possible, enter the wildcard character * into any text box. This will enable the administrator to view all the users that are accessible in one search output.

Procedure 10.1. To generate a user report:

1. Log in to the Managed File Transfer administration application as an administrator with the Reporting right.
2. Navigate to the Audit | Reporting | User Reports page.
3. On the User Reports page, configure the search attributes using the corresponding drop-down menus and text boxes. Select from the Add Filter drop-down menu to add a new search attribute. .
4. To configure the order of the search results, select from the drop-down menu the attribute to order the search results by and configure the following search options:
    a. Ascending - Select this option to display the search results in ascending order.
    b. Descending - Select this option to display the search results descending order.
    c. Number of Results Per Page - From the drop-down menu, select the number of results to be displayed on each page.
    d. Case Sensitive Search - Select this option to make the search sensitive to cases.
5. Select More to select which search variables to be included in the search output. Select all that apply.
6. Click Search.
7. To export the search results in a CSV file, select More and configure the download options:

a. Delimiter Character - Enter the character that will be used to separate each entry. A comma is suggested as the default option.

b. Quote Character - Enter the character that will be used to identify each variable output. Quotation marks are suggested as the default option.

c. Line Break Type - From the drop-down menu, select the line break type applicable to the Operating System used.

d. File Charset - From the drop-down menu, select the file encoding type applicable to the language used.

e. Click Download as CSV.

10.1.2. View Activity Reports

Administrators can generate reports of selected activities performed by all of the users for which administrators have the Reporting right. The search results will allow the administrator to view basic information for each instance of the activity performed in the selected month and year. The search results can only include the activities performed by users within the domains for which the administrator has rights. In the activity reports for exchanges and user authentication, the results can be grouped by time period or by domain.

Procedure 10.2. To generate an activity report:

1. Log in to the Managed File Transfer administration application as an administrator with the Reporting right.
2. Navigate to the Audit | Reporting | Activity Reports page.
3. On the Activity Reports page, configure the following activity report options:
    a. Report Type - From the drop-down menu, select a report type and configure the required options that correspond to the selected report type:
        - Usage Overview - If selected, the report type will display the overall basic usage report. There are no other options to configure for this report type.
        - Exchanges - If selected, this report type will display the number of exchanges made and the amount of data exchanged in either a given domain or across all domains within a selected time period.
        - Top Uploaders (in size) - If selected, this report type will display the users that have uploaded the greatest amount of files (in size not in number of files) within a selected time period either globally or within a selected domain..
        - User Authentication - If selected, this report type will display the total authentications made in either a given domain or globally within a selected time period.
    b. Covered Period - From the drop-down menu, select a coverage period and enter the respective date(s) in the corresponding text box(s).
    c. Domains - From the drop-down menu, select from which domains the search results should show. Only the domains that the administrator has Reporting rights over will be available for selection.
    d. Group By - From the drop-down menu, select a grouping mechanism for the search results to be displayed in.

4. Click the arrow icon and select Results Display Options to customize which search variables to be included in the search output. Select all that apply.
5. To export the search results in a CSV file, click the arrow icon and configure the download options:
    a. Delimiter Character - Enter the character that will be used to separate each entry. A comma is suggested as the default option.
    b. Quote Character - Enter the character that will be used to identify each variable output. Quotation marks are suggested as the default option.
    c. Line Break Type - From the drop-down menu, select the line break type applicable to the Operating System used.
    d. File Charset - From the drop-down menu, select the file encoding type applicable to the language used.
    e. Click Download as CSV.
6. Click Update.

10.2. Use the Audit Logs User Interface

Detailed information about the audit log events and the audit logs in general can be found in the EquiSign Managed File Transfer Audit Logs Guide. This section describes how to use the Audit Logs section of the Managed File Transfer administration application interface. In the Audit Logs interface, administrators can:

- Section 10.2.1, “Search for Log Entries”
- Section 10.2.2, “Download the Audit Log Files”

10.2.1. Search for Log Entries

The Managed File Transfer administration application allows administrators to use detailed search criteria to locate and display log entries.

Procedure 10.3. To search for log entries:

1. Log in to the Managed File Transfer administration application as an administrator with the Audit Logs right.
2. Navigate to the Audit | Audit Logs | Go to Audit Logs Interface.
3. On the Audit Logs Search page, accept the default search criteria to view all recorded logs or configure the following search criteria to search for specific log entries:
    a. Detail - From the drop-down menu, select the type of detail. In the text box, enter a known value for the detail.
    b. Actor - From the drop-down menu, select the type of actor. Select whether the actor corresponds with an identifier or a name, and in the text box, enter a known value for the actor.
    c. Title - From the drop-down menu, select a title that corresponds to the type of log entries that should be returned. The drop-down menu will include the titles from all

existing log entries and will expand as more actions on the Managed File Transfer administration application take place and are logged.

d. Tracking ID - From the drop-down menu, select a tracking item. In the text box, enter a known value for the item.

e. Type - From the drop-down menu, select one of the following search options:

   i. Action Records - to search all audit events

   ii. Alert Records - to search all alert events

   iii. All Records - to search all audit events and all alert events

f. Interval - To return log entries that were created during a specific time frame, enter the state and end dates to search between. Note that the interval applies to all other search criteria. For example, an administrator searching for a Detail of an application name would need to be sure that the interval dates are wide enough to include the date a log entry was created for the application name, such as the date it was created or modified.

g. Recipient - Select to value the recipient by either an Identifier or Name and enter into the text box a known value for the recipient.

h. Outcome - From the drop-down menu, select the outcome of the log entries that will be returned.

i. Number of Lines Per Page - Log results will be paged if they exceed the number entered here. Use the up and down arrows, or enter a value to configure the number of log entires to display on each page.

j. Module Name - From the drop-down menus, select the application name and then either admin or user to select the module name of the log entries to be displayed.

k. Attachment Purpose - From the drop-down menu, choose either Certificate or Exception to select the attachment purpose of the log entries to be returned.

4. Choose to Save Request, or click Search to send the request.

5. In the returned search results, to view more details for an audit log entry, select the Title, Actor, or Date of the entry. Select to View Detailed Log to view the full log entry.

10.2.2. Download the Audit Log Files

Administrators can download the log files or individual log file entries in either XML or CSV format.

1. Follow the instructions in Section 10.2.1, “Search for Log Entries”.

2. On the Log Search page, from the Other Options drop-down menu, select one of the download options and follow the associated instructions:

   a. To Download Results in XML Format, select the option.

   b. To Download Results in CSV Format, select the option. In the inclusion options, select the log entry details to include in the .csv file. Click Download.

   c. To download an individual log entry in a .xml file, follow the instructions in Section 10.2.1, “Search for Log Entries” and proceed to the full log entry page. In the Options box, select to Download XML Entry.

Chapter 11. Renew Web Server Certificates

When the MFT server application is initialized, as described in the "Initialize the Server Application" section of the MFT Server Installation and Upgrade Guide, the certificates required for the Apache Web Server of the MFT server application are signed. The Web Server certificates must be renewed before they expire. If any of the MFT server application's Web Server certificates are missing or expired, the MFT server application will not function correctly.

Procedure 11.1. To renew the Web Server certificates:

1. Log in to the server hosting MFT as the `root` user.
2. To start the configuration script, enter:

   `/opt/opentrust/mft/sbin/mft-config`.
3. If the "Do you want to run a simplified configuration" screen is displayed, choose Yes.
4. On the MFT Configuration screen, at the "Please choose a component to configure" prompt, choose Web Server and click OK.
5. On the Web Server screen, choose Manage Web Server Certificate and click OK.
6. On the Web Server Certificate screen, choose Renew Certificate and click OK.
7. On the Manage Web Server Certificate Renewal screen, choose a method for registering the certificate to be used for the Web server:
   - Create Certificate Private Key - Step 7.a: create a private key using the mft-config UI and then either export a CSR and import a signed certificate or generate a self-signed certificate
   - Import Certificate Private Key - Step 7.b: import a private key using the mft-config UI and then either export a CSR and import a signed certificate or generate a self-signed certificate
   - Import PKCS12 - Step 7.c: import a P12 file that contains the private key and already signed certificate

   a. If the choice is to generate a private key, on the Manage Web Server Certificate screen, to begin the process of creating a private key for the Web server's certificate, select Create Certificate Private Key and then click OK.

      i. On the Choose Key Size screen, choose the encryption strength to use for the private key and click OK.

      ii. On the Export CSR and Import Signed Certificate or Generate Self-signed Certificate screen, choose a signing method and follow the instructions in the appropriate substep.

         A. If the choice is to export the CSR to have it signed and then import the signed certificate:

            I. Select Export Certificate Signing Request and click OK.

            II. On the Select Directory screen, enter the directory path, without the file name, to the location the CSR should be exported to or accept the default selection of the `/tmp` directory and click OK.

III. On the CSR Exported screen, review the "The CSR has been exported as..." message containing the CSR file name and location and click OK.

IV. Leave the initialization procedure for the server currently being initialized, without closing the session, and use another application to sign the CSR. To use a pre-purchased Web server certificate instead of having using the exported CSR, contact an assigned Equisign technical representative for more information.

V. When a signed certificate has been obtained, return to the Export CSR and Import Signed Certificate or Generate Self-signed Certificate screen in the initialization procedure, select Import Signed Certificate and click OK.

VI. On the Enter Directory and File Name screen, enter the directory path location and file name for the signed certificate and click OK. The certificate must be in PEM format.

VII. On the Import Successful screen, click OK.

VIII. On the Manage Web Server Certificate screen, to return to the Web Server Initialization screen, click Back.

B. If the choice is to generate a self-signed certificate:

I. Select Generate Self-signed Certificate and click OK.

II. On the Generation and Import Success screen, at the "The self-signed certificate has been generated and imported." prompt, click OK.

b. If the choice is to import a private key before creating a certificate, on the Web Server Certificate screen, to begin the process, select Import Certificate Private Key and click OK.

i. On the Private Key Filename screen, enter the filepath and filename of the private key that has been copied to a directory on the server being initialized. The private key must be in PEM format without password protection. Then click OK.

ii. View the "The private key has been imported," success message and click OK.

iii. On the Export CSR and Import Signed Certificate or Generate Self-signed Certificate screen, choose a signing method and follow the instructions in the appropriate substep.

A. If the choice is to export the CSR to have it signed and then import the signed certificate:

I. Select Export Certificate Signing Request and click OK.

II. On the Select Directory screen, enter the directory path, without the file name, to the location the CSR should be exported to or accept the default selection of the `/tmp` directory and click OK.

III. On the CSR Exported screen, review the "The CSR has been exported as..." message containing the CSR file name and location and click OK.

IV. Leave the initialization procedure for the server currently being initialized, without closing the session, and use another application to sign the CSR. To use a pre-purchased Web server certificate instead of having using the exported CSR, contact an assigned Equisign technical representative for more information.

V. When a signed certificate has been obtained, return to the Export CSR and Import Signed Certificate or Generate Self-signed Certificate screen in the initialization procedure, select Import Signed Certificate and click OK.

VI. On the Enter Directory and File Name screen, enter the directory path location and file name for the signed certificate and click OK. The certificate must be in PEM format.

VII. On the Import Successful screen, click OK.

VIII. On the Manage Web Server Certificate screen, to return to the Web Server Initialization screen, click Back.

B. If the choice is to generate a self-signed certificate:

I. Select Generate Self-signed Certificate and click OK.

II. On the Generation and Import Success screen, at the "The self-signed certificate has been generated and imported." prompt, click OK.

iv. For help with this process, contact an assigned Equisign technical representative.

c. If the choice is to import a PKCS12 instead of importing or generating a private key, on the Web Server Certificate screen, select Import PKCS12 and then click OK.

i. On the PKCS12 Filename screen, enter the filepath and filename of a PKCS12 file that has been copied to a directory on the server being initialized. Then click OK.

ii. On the PKCS12 Password screen, enter the password of the PKCS12 file that is being imported. Then click OK.

iii. On the Success screen, at the "The private key and certificate have been imported." success message, click OK.

d. After being returned to the Manage Web Server Certificate screen, to return to the Web Server Configuration screen, click Back.

8. This step is optional. The Web server's certificate chain file (the issuing CA's certificate and the intermediate CA's certificates up to a root CA) can be imported as a bundle. The Web server's certificate chain is made available to HTTPS clients to verify the Web server's certificate, up to one of their trusted root CAs. The Web server certificate's chain file is usually provided by the CA that generated the Web server's certificate. For example, the chain is one of the attachments in the default email templates for delivering a server certificate in PKI.

   To import a certificate chain file, on the Manage Web Server Certificate screen, select Import Certificate Chain File and click OK. On the Certificate Chain Bundle Filename screen, enter the filepath and filename of the certificate chain bundle that has been copied to a directory on the server being initialized. The certificate chain bundle must be in PEM format. Then click OK, view the "The certificate chain bundle has been imported," success message, and click OK again.

9. After being returned to the Web Server Configuration screen, to return to the "Please Choose a Component to Initialize" screen, click Back.

10. On the "Please Choose an Item to Configure" screen, click Exit.

11. When prompted, to apply the changes, enter:

```
service mft restart httpd
```